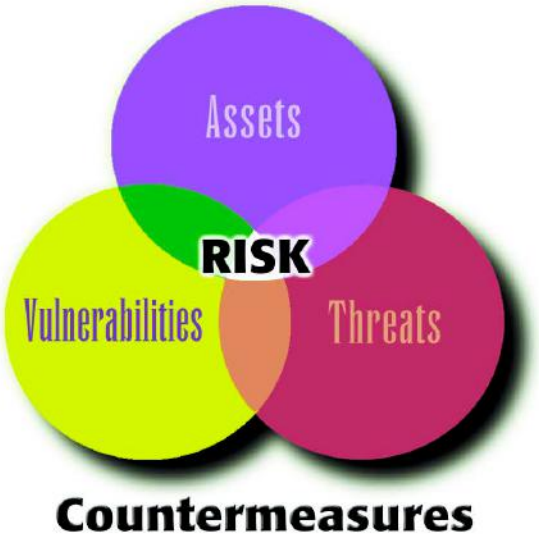
# Analytical Risk Management

# Analytical Risk Management




## A Course Guide for Security Risk Management

January 2000

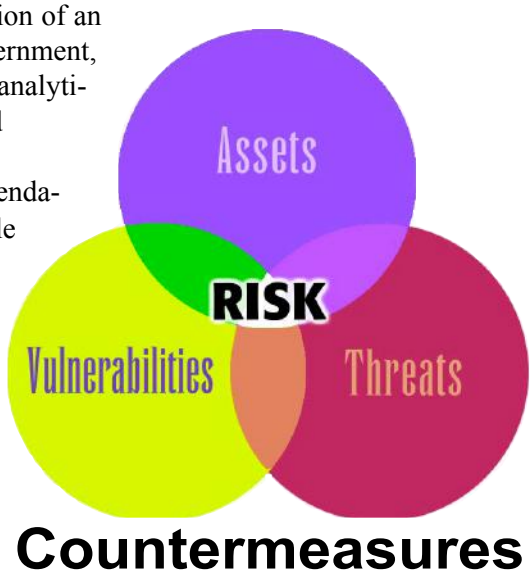
# Table of Contents

# Table of Figures

# About This Guide

This guide is the result of a project sponsored by the US Government. This guide was developed for the US Government under contract by Booz·Allen and Hamilton, Inc. The project grew out of a concern shared by senior leadership and security professionals within the Intelligence Community that the security risk management process needed to be more clearly defined. The purpose was to establish a process for security specialists and their customers to understand risk management concepts and accomplish risk management tasks in a more efficient and effective manner.

The concept for this guide was developed after a thorough review was conducted on existing views and current approaches to security risk management. Security professionals from both government and industry were interviewed to identify what worked, and what didn't work, with respect to risk assessment techniques. Upon completion of an internal validation of the process within the US Government, and based on feedback from course participants, the analytical risk management framework presented in the 2nd edition of this guide has successfully proved:




- Useful in providing assessments and recommendations of value to managers who are responsible for accepting risks, planning, and funding security programs
- Useful in both classified and unclassified environments
- Useful in conducting both qualitative and quantitative assessments
- Appropriate for various types of sites
- Capable of providing accountability
- Adaptable for use and integration with existing risk assessment tools
- Flexibly structured to permit use of existing security documentation as input to a risk assessment framework
- Useful as an information source for a security staff and customers
- Not overly labor intensive for the user.

As a final note, it should be stressed that risk assessment methods as a means to identifying countermeasure options are not beneficial if they are presented as excessively detailed, overly quantitative, or if they are not integrated into the management decision-making process. It is the intent of this guide to encourage users to select and apply analytical tools that are appropriate for their tasks and in the context of their customer's decision-making system. Excessive formalization that tends to over-complicate the risk management process should be avoided.

# The Analytical Risk Management (ARM) Process

We can and must provide a rational, cost-effective and enduring framework using risk management as the underlying basis for security decisionmaking.
— From *Redefining Security*, a report by the DOD/DCI Joint Security Commission, 1994

The task of protection is increasingly complex with the rapid political, social, economic, and technological changes that are taking place today. At the same time, resources for security are more constrained. The purpose of this guide is to provide a systematic approach to acquiring and analyzing the information necessary to support decision makers in the protection of assets and the allocation of security resources. It is designed as a tool to help security managers, analysts, and technicians in the day-to-day performance of their jobs — supporting the planning, implementation, and evaluation of risk-based security strategies.

**Risk Management** is "the process of selecting and implementing countermeasures to achieve an acceptable level of risk at an acceptable cost." The **analytical risk management (ARM) process** outlined in this guide can be tailored and applied to any security analysis task. This document provides examples focused primarily on facilities — or site — protection and the assets contained within a facility or specified area. The process includes the following activities:

- Collection and evaluation of accurate and detailed information regarding the
  - Nature and value of the assets — Step 1
  - Degree of a specific type of threat — Step 2
  - Extent of the related vulnerabilities — Step 3
- Identification and evaluation of risks — Step 4
- Cost—benefit analysis of countermeasures to mitigate specific, selected risks — Step 5

These activities should be conducted on a continuing basis because risk management is a dynamic process requiring the monitoring of changes to asset value, threat, and vulnerability. Where significant risks have been accepted, it is important to include contingency planning as part of the risk management process. Where there are residual risks—risks not addressed—plans should be prepared to address them at a later date or as the security environment changes.

The ARM methodology uses a systematic approach. It provides structure, record-keeping, and objectivity within each step of the process. Each step outlined above is broken down further into sub-steps which are described in this guide. Since risk assessment is not an exact science, it is important to maintain an audit trail that tracks the expert opinions and judgments made during each step. This documented audit trail can be provided to the decision maker for review, and can be used as a baseline for follow-on or future analyses and assessments.

In conducting complex risk assessments, the effective application of this process integrates the skills, knowledge, and experience of a variety of specialists, as well as the customer and the security analyst. It is important for the analyst to know when and how to solicit information and advice from other professionals. Using a team approach helps ensure that the customer is provided with credible and defensible recommendations that are based on objectively collected data, rather than on the judgment or memory of a single expert.

Risk management includes cost as a major variable in the decision making process. Identifying and prioritizing security requirements is especially important when resources are limited and can only be allocated against what we determine to be our most critical needs. With this ARM model, the goal of security planning shifts from achieving maximum feasible security

to achieving maximum effectiveness in the allocation of limited resources. Our objective is to do the right things right.

The five step process depicted below is an *iterative* versus *sequential* process. That is, each step may yield new information which affects the information developed earlier. Data gathered during each step of this process should be documented and maintained for further analysis and presentation to the customer as backup data for proposed recommendations and alternatives.

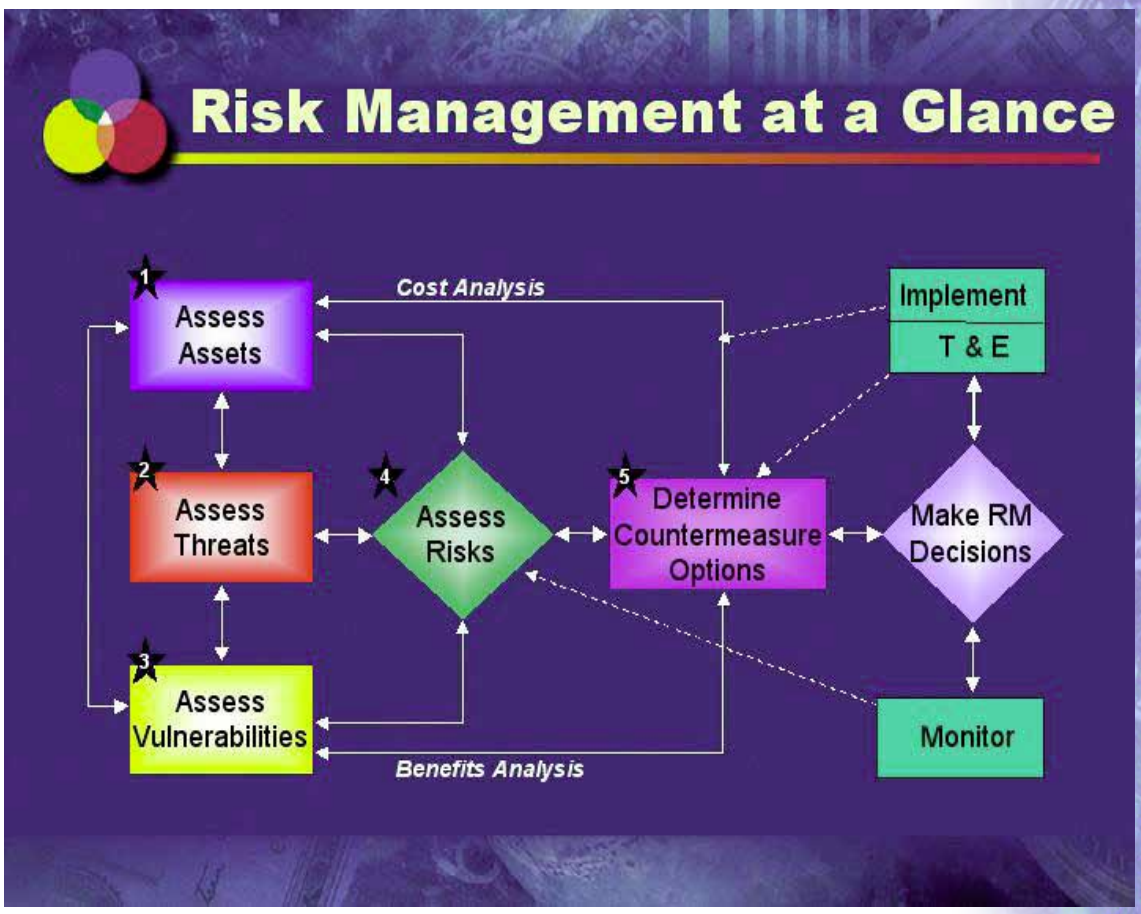



*Figure 1: Analytical Risk Management Process Diagram*

"The process begins with an assessment of the value of assets, the degree of a specific threat, and the extent of the vulnerabilities. These three factors determine risk. A decision is then made as to what level of risk can be accepted and which countermeasures should be applied. Such a decision involves a cost-benefit analysis, giving decision makers the ability to weigh varying security risk levels against the cost of specific countermeasures."

Noted on the figure are additional elements necessary to the risk management process. Providing countermeasure options with their rational must be followed by decisions made by those in authority. With decisions made to accept countermeasure recommendations, implementation actions are taken following careful planning. Once countermeasures are in place, they must be tested and evaluated (T&E) to ensure they are effective. As noted earlier, a monitoring system should be established to detect any changes in Assets, Threats, and/or vulnerabilities which might change our risk assessment.

The arm methodology serves as a tool for the security practitioner by offering a structure for organizing related material and focusing their knowledge and expertise.

— From *The Diplomatic Security Risk Management Policy*

# Outline of Analytical Risk Management Steps

## Step 1. Identify assets and loss impacts

1.1 Determine valued assets requiring protection
1.2 Identify undesirable events and expected impacts
1.3 Value/prioritize assets based on consequence of loss

## Step 2. Identify and characterize the threat

2.1 Identify threat categories and potential adversaries
2.2 Assess intent and motivation of adversaries
2.3 Assess capability of adversaries
2.4 Determine frequency of threat-related incidents based on historical data
2.5 Estimate degree of adversary threat to each valued asset and undesirable event

## Step 3. Identify and analyze vulnerabilities

3.1 Identify potential vulnerabilities related to valued assets and associated undesirable events
3.2 Identify existing countermeasures and their level of effectiveness in reducing those vulnerabilities
3.3 Estimate degree of vulnerability of each valued asset and threat

## Step 4. Assess risk and determine priorities for asset protection

4.1 Estimate degree of impact of an undesirable event relative to each valued asset
4.2 Estimate likelihood of attack by a potential adversary
4.3 Estimate likelihood that a specific vulnerability will be exploited
4.4 Determine your relative degree of risk [Risk = {expected Impact} x {likelihood of successful attack (Threat x Vulnerability)}] — R = I x(TxV).
4.5 Identify unacceptable risks and establish risk mitigation priorities

## Step 5. Identify countermeasures, costs, and tradeoffs

5.1 Identify potential countermeasures principally to reduce vulnerabilities
5.2 Identify countermeasure capability function and effectiveness and effectiveness — its benefit in terms of risk reduction
5.3 Determine degree of risk reduction (the benefit) provided by the countermeasure
5.4 Identify countermeasure costs
5.5 Conduct countermeasure cost-benefit and trade-off analyses
5.6 Prioritize options and prepare recommendations for decision maker

# Definition of Key Terms

For the purpose of this guide, the following definitions of key terms are used. These terms are consistent with those used by the intelligence and security communities and with the evolution of the analytical risk management process described in this guide.

### Risk Management:

The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

### Risk:

Risk is the potential for damage to, or loss of an asset. The level of risk [R = I (impact) x T(threat) x V(vulnerability)] is a combination of two factors:

1. The value placed on that asset by its owner and the consequence,of an undesirable event on that asset — the impact (I) in terms of adverse effect or loss or damage to the asset.
2. The likelihood that a specific vulnerability (V) will be exploited by a particular threat (T).

### Asset:

An asset is any person, facility, material, information, or activity which has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets may be categorized in many ways. Among these are:

- People
- Information
- Equipment
- Facilities
- Operations/Activities

### Impact:

Impact is the amount of loss or damage that can be expected, or may be expected from a successful attack of an asset. Loss may be monetary but may also include political, morale, operational effectiveness, etc. impacts.

### Threat:

Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Sources of threats my categorized as:

- Foreign Intelligence Service
- Insider
- Criminal (Outsider)
- Terrorist
- Environmental
- Foreign Military

## Adversary:

An adversary is an individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. These include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, and private interests.

## Vulnerability:

Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can result from, but are not limited to, the following: building characteristics; equipment properties; personal behavior; locations of people, equipment and buildings; or operational and personnel practices.

## Risk Assessment:

Risk assessment (R) is the process of determining the likelihood of an adversary (T) successfully exploiting a vulnerability (V) and the resulting degree of damage or impact (I) on an asset. A risk assessment provides the basis for rank ordering risks and thus establishing priorities for the application of countermeasures. Thus, the formula $R = I \times (T \times V)$ is used.

## Countermeasures:

A countermeasure is an action taken or physical equipment used principally to reduce or eliminate one or more vulnerabilities. Countermeasures may also affect the threat (intent and/or capability) as well as an asset's value. The cost of a possible countermeasure may be monetary but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

## Cost Benefit Analysis:

A cost-benefit analysis is the part of the management-decision making process in which the costs and benefits of each countermeasure alternative are compared and the most appropriate alternative is selected. Costs include the cost of tangible materials, and also the on-going operational costs associated with countermeasure implementation. Benefits are expressed in terms of the amount of risk reduction based on the overall effectiveness of the countermeasures with respect to the assessed vulnerabilities.

# Step 1: Identify Assets and Loss Impacts

The first step in the analytical risk management process, shown in Figure 2, is to identify the valued assets requiring protection. Recognizing that not all assets and activities warrant the same level of protection, you will need to identify which assets need safeguarding and to assess their relative value or importance. Asset value need not be assessed in dollars; however, the cost of the countermeasures used to protect assets must be reasonable in relation to the overall value of the assets to be protected. Assets can be valued relative to the impact (I) of their potential loss; for example, the impact that the loss an asset might have on human lives or national interests. Understanding that assets may have value to an adversary that may be different from their value to us is a key factor in this process. If an adversary places a high value on our asset, the likelihood increases for that asset becoming a target.

During this step, the risk analyst conducts a preliminary survey of assets and then determines which of the assets are most value. A risk analyst will review findings related to assets again in Step 2 — identify and characterize specific threats and adversaries.

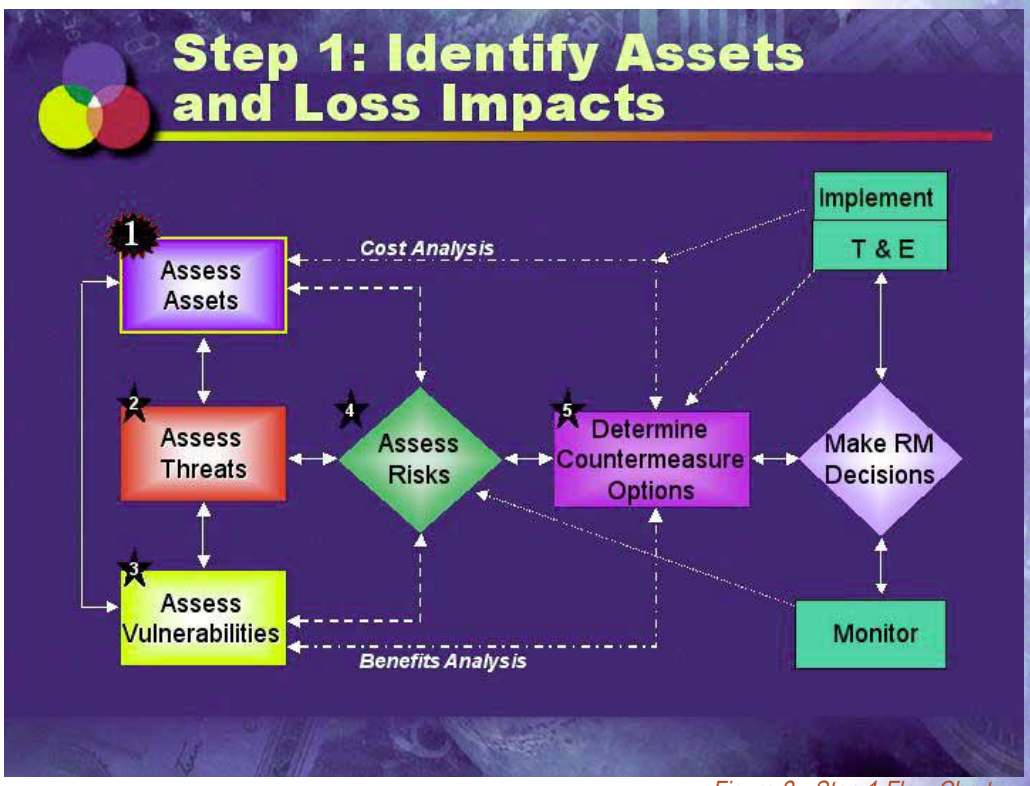



*Figure 2 - Step 1 Flow Chart*

**Asset**: Any person facility, material, information, or activity which has a value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets may be categorized in many ways.

## 1.1 Determine Valued Assets Requiring Protection

Using the categories listed below will help identify the general types of assets relevant to an analysis. Specific assets of concern to a customer then can be determined within each of these categories. The five basic categories include:

- People
- Equipment/Materials
- Information
- Facilities
- Activities/Operations

Examples within each of the five categories are provided below. The subcategories below may be used as a guide to preparing more specific questions for asset surveys:

## 1. People

American Citizens
- Government Agency Personnel
- Covert Personnel
- Contractors/Vendors
- Military Personnel
- Dependents/Visitors

Foreign Nationals
- Foreign Service Nationals (FSNs)
- Government Officials
- Contractors/Vendors
- Foreign Military Personnel
- Dependents/Visitors

## 2. Information

Classified
- Sensitive Compartmented Information
- Top Secret
- Secret
- Confidential
- Sensitive Sources
- Sensitive Methods

Unclassified
- System Designs
- Intellectual Property
- Patents
- System Capabilities/Vulnerabilities
- Sensitive Financial Data
- Personnel Rosters
- Organizational Diagrams
- Phone Book

## 3. Equipment/Materials

- Transportation Equipment/Vehicles
- Maintenance Equipment
- Operational Equipment (Office, Field)
- Communications Equipment
- Security Equipment
- Weapons (Conventional, Nuclear, Biological)
- Automated Information Systems and Equipment
- Production Materials

## 4. Facilities

Domestic Facilities (Gov't and Industry)
- Headquarters
- Field Offices/Administrative Buildings
- Training Facilities
- Contractor Facilities
- Storage Facilities
- Production Facilities
- R&D Laboratories
- Power Plants
- Parking Facilities
- Aircraft Hangars
- Residences
- Operational Facilities

U.S. Facilities Overseas
- Embassies
- Stations/Bases
- Military Installations
- Other Government Sites
- Industry Sites
- Residences

## 5. Activities/Operations

Intelligence Collection/Analysis
Sensitive Movement of Operations/Personnel/Property
VIP Protective Operations
Conduct of Sensitive Training
Communications/Networking
Military Operations
Clandestine Operations
Conduct of Sensitive Negotiations
Interception of Adversary Operation
RDT&E and Sensitive Technology
Production of Sensitive Technology
Protection of Nuclear/Biological /Chemical Materials
Protection of Weapons, Explosives, and Equipment

## Gathering Asset Data

You can gather information about valued assets from a variety of sources, including:

- Site Personnel
  - Facility Manager
  - Chief of Operations
  - Chief of Security
  - Logistics Personnel
  - Other Facility Staff
  - Facility Customers
  - Construction Contractors
  - Maintenance Staff
- Existing security plans, security survey/audits
- Rosters of classified documents, and personnel located at a particular site
- Open source information

The "asset owners," often your customers, are generally the most knowledgeable about the assets in need of protection. They generally have the best idea as to which assets are the most sensitive and valuable. Plan to conduct in-depth interviews and guide them through the process of identifying the most value assets. You should be familiar with the customer's mission and activities before conducting the interviews. A tour of the site focusing on the location of assets should also be conducted before, or as a part of, the interview process.

### Structured Asset Survey

1. **What critical mission activities/operations take place at this site? Describe.**
2. **Who are the facility personnel, tenants, customers, and visitors? What relationship do they have to the critical mission activities/operations?**
3. **What critical/sensitive information (both classified/unclassified) are located at the site?**
4. **What critical/valuable equipment is located at the site? Why is it critical/valuable?**
5. **Where are the assets located?**
6. **What do you view as undesirable events to your assets? Describe the expected impact if the event were to occur.**

*Figure 3: Sample Asset Survey Questionnaire*

To gather asset information in an objective manner, you should develop a structured interview guide specifying the topics to be covered during the interviews with site personnel. Remember, the purpose of these interviews is to identify valued assets and the expected impacts if those assets are compromised. You want to ask questions in an objective and unbiased manner. Initial questions should be open-ended, as shown in Figure 3 to encourage uninhibited discussion. As information is revealed more probing questions should be asked to ensure that complete

and accurate information is elicited. During Step2, threat data is reviewed to determine specific adversaries with the intent, capability and history to target our assets. During Step 2, a determination also should be made from an adversaries perspective in valuing our assets. If an adversary values your asset(s). More than you do, consider re-evaluating your asset and it's potential loss. Revise conclusions reached in Step 1 accordingly.

## 1.2 Identify Undesirable Events and Expected Impacts

During this phase of the analysis, risk analysts identify specific undesirable events and the potential impacts if those undesirable events were to occur. For example, if certain information pertaining to the identity of clandestine personnel needs to be protected; the undesirable event would be an adversary obtaining this information. The impacts could be the asset's arrest, death, doubling, etc.

Some of the key questions an analyst needs to ask when assessing loss impacts of any asset are: How does obtaining this information help the adversary attain its goals? What would we lose? What would the adversary gain? Is this asset still valuable to us once it has been compromised? What did it cost us to develop this asset? What is the impact on people's lives, the economy, the environment, and other aspects of national security?

| Valued Assets to be Protected | Potential Undesirable Events & Impact |
|---|---|
| Intelligence Officer | • Terrorist attack results in assassination/kidnapping<br>• Exposure of affiliation by insider results in surveillance and arrest by hostile intelligence service |
| Satellite System Capability | Insider leak of info results in denial/deception by target |
| Communications Relay | Sabotage results in denial of communications |
| Automated Information Systems | Stand-off attack (hacking) results in unauthorized access to classified information |

*Figure 4: Sample Worksheet: Identifying Assets and Related Undesirable Events & Impacts*

Once the consequences (the impacts) have been determined for each potential undesirable event, the degree of importance of each asset can be rated or ranked relative to the other assets. The question the analyst is trying to answer is: "How does the need for protection of this asset compare with the other valued assets?" The asset owner should be involved in the process of evaluating the loss impact and relative value of the asset. If the assessment is made by a security analyst, the results should be validated by the asset owner. Figure 4 shows a suggested worksheet for preliminary analyses.

Undesirable events result in undesirable losses and are described by crafting undesirable event statements. Examples of such statements are shown at Figure 5. The arrows shown in the figure represent the words "result in."

## 1.3 Value/Prioritize Assets Based on Consequence of Loss

Understanding the nature and the value of the assets that one believes requires protection allows one to make more rational decisions about related vulnerabilities, and the allocation of protective countermeasures. It also helps ensure that the most valued assets will be protected and resources allocated where they will have the greatest positive impact. During this part of Step 1 a risk analyst will make estimates of the degree of impact of undesirable events on critical assets. It is important to recognize that the value of people, information, and activities is difficult to quantify in terms of dollars. Therefore, it may be more appropriate to provide a linguistic and/or numerical scale to express the consequence of loss than it would be to quantify impacts in dollars.

## Assessing Loss Impacts

The loss impact (I) can be quantified as a relative rating based on the best available information from the sources mentioned above (see "Gathering Asset Data"). To determine the relative degree of impact (I) if an asset were to be compromised in some way, a scale should be developed to promote consistent ratings of impact levels. Example Impacted Rating Criteria that may be used to assess the impact of asset loss are shown at Figure 6. You may, of course, create your own impact or risk scales as outlined in Appendix A.

The linguistic impact rating criteria, defined in the chart below, can be used when a monetary impact assessment is not required, or is too difficult to determine. If more granularity is required, a numeric scale from 1-100 can be used to provide a relative ranking of potential losses.

The sample chart, shown in Figure 7, can be used to capture information pertaining to critical assets and the level of impact that undesirable events may have on those assets.

The product of this phase of the analysis should be a description of the undesirable events associated with each critical asset and an impact assessment describing the consequence of loss if the undesirable event were to occur.

*Note:* See Step 4 for a description on how to establish relationships between linguistic and numerical scales.


*Figure 5: Undesirable Event Statements*

### Impact Rating Criteria

Critical: Indicates that compromise to the asset targeted would have grave consequences leading to loss of life or serious injury to people or mission failure. (Numerical Rating Scale = 50 to 100)

High: Indicates that a compromise to assets would have serious consequences resulting in loss of classified or highly sensitive data or equipment/facilities that could impair operations for an indefinite amount of time. (Numerical Rating Scale = 13 to 50)

Medium: Indicates that a compromise to the assets would have moderate consequences resulting in loss of confidential, sensitive data or costly equipment/facilities that would impair operations for a limited period of time. (Numerical Rating Scale = 3 to 13)

Low: Indicates little or no impact on human life or the continuation of operations. (Numerical Rating Scale = 1 to 3)

*Figure 6: Impact Decision Matrix*

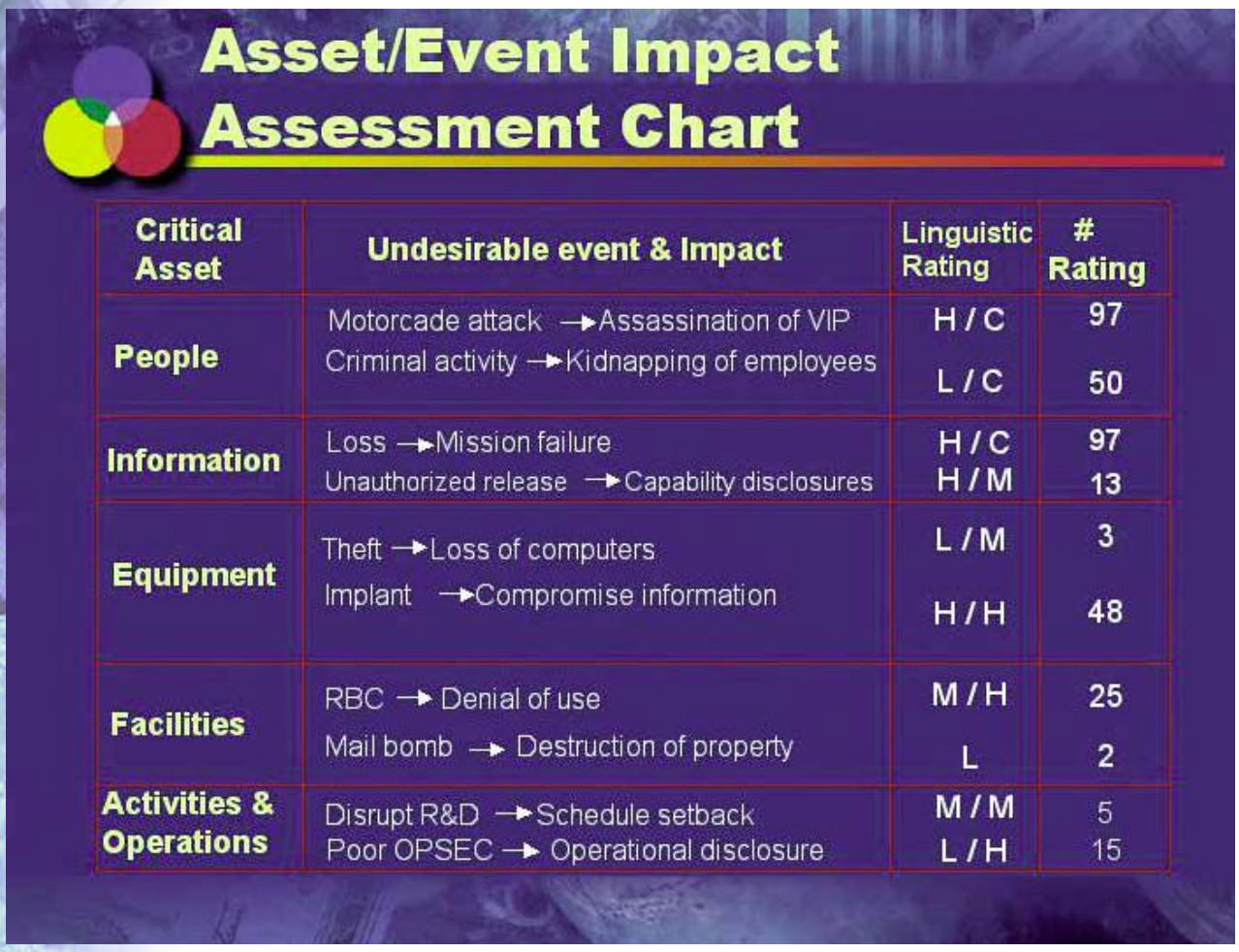
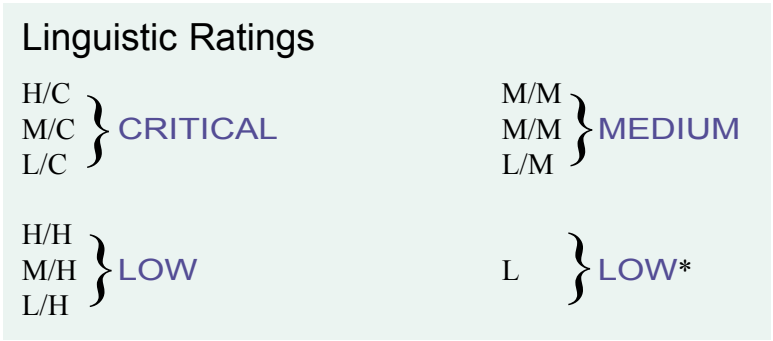



*Figure 7: Asset Loss Impact Summary*

*Note: Also See Appendix A




Linguistic Categories

# Step 2: Identify & Characterize the Threat to Specific Assets

The second step in the analytical risk management process, shown in Figure 8, is to understand the specific threats and adversaries that relate to the assets identified in the previous step. Understanding threats requires an understanding of the adversaries' intentions and motives, as well as their capability to compromise critical assets. Because access to this type of information is often limited, this is generally the weakest link in the overall risk assessment process. The process outlined in this step will not guarantee the risk analyst will obtain all the information needed to thoroughly assess threats; however, it will provide a framework for collecting threat data and allow the risk analyst to track and recognize which judgments are based on facts, and which are based more on assumptions or speculation.

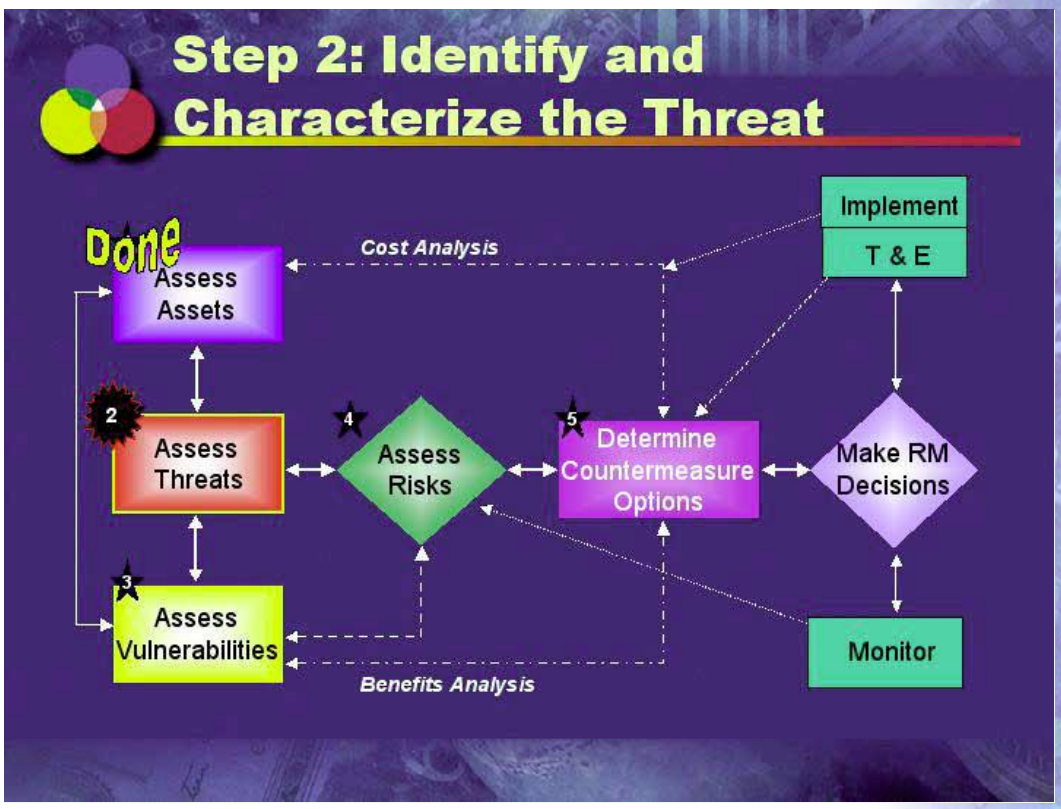



*Figure 8: Step 2 Flowchart*

## 2.1 Identify Threat Categories and Potential Adversaries

During this step the risk analyst identifies and lists the potential threats, and any known or potential adversaries, that could put critical assets at risk. The analyst reviews the list of potential threat categories and estimates the potential threats and identified adversaries in terms of intent, capability, and history. It is important to develop criteria that allows one to rate threats consistently using the same criteria as other members of the team. Threats may be broken down into the following categories:

1. Foreign Intelligence Service
2. Terrorist
3. Insider
4. Criminal
5. Environmental
6. Foreign Military.

**Threat:** Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets. Threat is an attribute of the adversary.

**Adversary:** An adversary is an individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to critical assets. These include intelligence services of the host nation or third party nations, political or terrorist groups, criminals, and private interests.

Listed below are some examples of specific types of threats within each of the major categories. Of course, example cited may pertain to move than one category — e.g., Terrorists might use HUMINT, SIGINT, etc. to collect information about their target. These examples can help a risk analyst brainstorm and identify undesirable events that could occur at a specific site:

1. Foreign Intelligence Service Threat
   - Human Intelligence (HUMINT) (e.g., recruitment, blackmail, surreptitious entry, phone taps, bugs, unauthorized computer access, etc.)
   - Signals Intelligence (SIGINT) (e.g., intercept/exploit communications, computer data, TEMPEST, etc.)
   - Imagery Intelligence (IMINT) (e.g., overhead imaging, hand held photography, etc.)
   - Measurement and Signature Intelligence (MASINT) (e.g., collecting, analyzing, effluent or debrey, etc.)
   - Open Source Intelligence (OSINT) (e.g., Websites, public releases, newspapers, etc).

2. Terrorist Threat
   - Assassination
   - Bombing
   - Kidnapping
   - Radiological, Biological, Chemical attacks
   - Nuclear attacks
   - Stand-off weapons attacks/Raids

3. Insider Threat
   - Malicious acts by disgruntled personnel (violence, sabotage)
   - Espionage/theft of classified material for adversary
   - Unauthorized disclosure of classified material
   - Theft of property
   - Inadvertent loss of classified material

4. Criminal Threat (Outsider)
   - Violent acts against people
   - Theft/destruction of property
   - Mob Violence
   - Hacking/Cracking of Computer Systems

5. Environmental Threat
   - Fire
   - Storm
   - Pollution
   - Earthquake
   - Flood

6. Military Threat
   - Nuclear
   - Radiological/Biological/Chemical
   - Conventional
   - Unconventional
   - Information Warfare

## Types of Adversaries

Adversaries can be classified in a number of ways. Here are some ideas that may be useful:

**Outsider:** An adversary who does not have access to privileged knowledge of a facility, activity, etc.

**Insider:** An adversary who has special privilege and access.

**Collusion** is when an outsider and an insider work together.

Adversaries can be distinguished in terms of their motivations or intentions. Types of adversaries of concern will generally fall into one of the following categories.

**Terrorist:** Motivated by their cause — religious, political, other.

**Criminal**: Motivated by greed. Money is the primary goal.

**Psychotic:** Motivation is unclear. Some sort of personal or job pressure has made them snap. "Suicide-by-cop" is a vexing problem. Individuals who seek death but are not able to take their own lives are compelled to die at the hands of another. They are often attracted by the very countermeasures placed to discourage the rational adversary.

**Disgruntled Employee:** Motivated by the desire to get even with the organization/company that wronged them.

**White Collar Criminal:** Motivation is the same as any criminal, but the adversary is an insider.

**Foreign Agent:** Motivated by money, ideology, compromise, ego, or some combination of these.

## Gathering Threat Data

The collection and analysis of threat information is critical to the risk assessment process. In order to make valid assessments of threats it is essential to understand as much as possible about each specific adversary. This can be a difficult and time-consuming process. Fortunately, recent trends in information technology and an evolving culture of greater information-sharing in the security community are making the process of threat analysis easier than ever before.

The collection of threat information is most effective when it is a continuous process. While it is possible for the analyst to collect threat information just prior to each individual analysis, this "as needed" approach is not as effective or efficient as building files of relevant information over a longer period of time. By building topic files and filling them with threat information as it becomes available, the analyst can create an resource for future analyses. This approach also helps improve the analyst's overall awareness of the threat environment, and may reduce the need for time-consuming pre-analysis research prior to each project. This approach also helps you develop the "right questions" when seeking input from others.

Information resources can be divided into two types: those that provide unclassified or "open-source" information, and those that provide classified information. Depending on the analysis, one or the other source may provide the necessary threat information, although a combination of both is often used.

It is important for the analyst to understand the difference between finished intelligence and reporting. Finished intelligence is a product that is derived from a collection of information, its processing and subsequent analysis and dissemination by one or more subject-matter experts. Information reporting, whether classified or unclassified, is information that has been collected and reported — but not evaluated by a subject-matter expert. As such it is subject to greater inaccuracies, misinterpretation and misinformation. In cases where unevaluated reporting must be used, the analyst should carefully consider the source of information and verify their conclusions with subject-matter experts whenever possible. The analyst should also attempt to use multiple independent sources to verify the information.

## Sources of Classified Threat Information

The analyst's own files should always be the starting-point in conducting threat research. Once that resource has been exploited, the risk analyst should consult with his/her own organization's internal threat resources. In many organizations this will include the resident Counterintelligence Representative. The CI Representative provides the focal-point between the organization and external intelligence and law enforcement organizations that provide threat information. Bringing the CI representative into the research effort early may save time and reduce frustration later on.

In addition to CI Representatives, internal experts can provide valuable threat information. Conducting interviews or hosting focus groups of experts with access to threat information often yields the most specific and useful information available.

Another valuable source of finished threat intelligence is information that is published by the various organizations of the intelligence community. Analysts can get on mailing lists for written products produced by the Counterterrorist Center and the National Counterintelligence Center. These written analyses provide some of the most thoroughly researched and analyzed threat information available on terrorism and counterintelligence threats.

Another increasingly useful resource for finding classified threat information is the variety of Internet-like computer networks that now exist throughout the intelligence and defense communities. One such network, InteLink, provides a intelligence community wide network for the sharing of classified intelligence information. Similar networks are available, on smaller scales, in many of the individual government organizations. Skillful searching of these networks can yield significant amounts of useful threat information.

Finally, analysts should not neglect their own internal documents and reports for threat information. For example, security surveys, old analyses and security incident reports often contain useful information about threats which have resulted in incidents or concerns in the past. These often provide excellent quantitative and anecdotal information that can be used in risk assessment tasks.

## Sources of Unclassified Threat Information

There are many possible sources of unclassified threat information. Perhaps the most prevalent of these is the mass media. From newspapers to the evening news, information about incidents, which represent the threats to our assets, is written, reported and broadcast every day. While such information should not be taken as factual and unbiased, it can provide the starting point for further research.

The US Government is the largest publisher in the world. Through the US Government Printing Office, the Internet, and individual agencies and Departments, the United States disseminates information on almost every imaginable topic of interest. Included among this information are a number of documented reports about threats to our safety, economic competitiveness and national security. All of this is free to use for anyone willing to seek it out.

Official speeches and testimony are another excellent example of thoroughly evaluated intelligence that is then made available to the public in unclassified form. For example, directors of agencies, the CIA and FBI in particular, give frequent updates to Congress on issues like terrorism, hostile intelligence collection and a variety of military threats. These speeches are usually available on a variety of agency-sponsored and privately sponsored Internet sites.

In addition to Internet sites, a number of commercial service providers have excellent resources for the security professional to use. For example, Lexis-Nexis (for a price) provides users the ability to search thousands of newspapers and periodicals by word, date, or other simple but useful techniques.

Special interest groups and professional associations also provide valuable and up-to-date information that is useful for security professionals. Resources which provide excellent Internet

sites which cover a range of security threat information are the Computer Emergency Response Team (CERT) and the National Security Institute (NSI). Another Internet site that is rapidly becoming a valuable resource is the Extranet for Security Professionals (ESP). Still another site is the OPSEC Professionals Society which archives their daily Z-gram that highlights current news and other resources of interest to security professionals.

### The Role of "Centers" in Disseminating Threat Information

The requirements for getting information from those that collect and/or analyze it to those who need it has always been a problem. One approach the community has taken to solve this problem is to create "centers." The centers coordinate activities, perform analysis and disseminate information as defined in their charters. Some are staffed primarily by the host organizations, but others are staffed by representatives of the national-level intelligence agencies, federal law enforcement organizations, and the armed services. Below are the names of a few of the centers which cover topics of interest to security professionals.

- Counterterrorist Center — A DCI center, staffed by representatives from the Intelligence and Law Enforcement communities.
- National Counterintelligence Center — A national center set-up after the Ames case. Part of its role is to coordinate the dissemination of counterintelligence threat information to security professionals.
- Counternarcotics Center — A CIA/Directorate of Intelligence center which coordinates analysis of counternarcotics issues.
- Center for Security Evaluation — A joint CIA-Department of State center designed to coordinate the security efforts of those two organizations.

## 2.2 Assess Intent and Motivation of the Adversary

Intent is determined for the most part by inference. The analyst will infer intent through a set of questions regarding the adversary. For example, "Does the adversary have a current or projected need for the asset we seek to protect? Do they seek to deny us the use of the asset? Have they demonstrated an interest by targeting similar types of assets? Are they trying to develop a similar asset? Do they know the asset exists and where it is located?"

Some believe that capabilities only should be considered when doing a threat assessment. This approach, however, leads to the development of a risk avoidance strategy since resources might be used for protecting assets from adversaries who have no interest in them. Therefore, the degree of overall threat is considered lower if there is no perceived intent on the part of the adversary. To determine the intent and what motives an adversary, look closely at an adversary's ultimate goals and objectives, as well as specific events that might trigger the adversary to act. In addition to the questions above, one should consider the following:

- What are the specific goals and objectives of the adversary?
- What does the adversary gain by achieving these goals?
- Can the adversary achieve any of these goals or objectives by exploiting our assets?
- How will the adversary obtain its goals through exploiting our assets?
- Is it the adversary's intent to obtain, damage, or destroy the asset?
- Are there other means for the adversary to obtain its goals? Are the other means easier?
- What is the probability that the adversary will choose one alternative means over another?
- What motivates the adversary to pursue its objectives?
- What specific events might provoke the adversary to act?

- What might the adversary lose in attempting to exploit our assets? Would that loss be a rational tradeoff from the adversary's perspective?
- To what degree is the adversary motivated to use its capability?

Figure 9 depicts a sample chart that can be used to document facts or assumptions related to the intentions and motives of your adversaries. For each positive (yes) statement, the risk analyst documents and supports with specific reasons.

| Adversary<br>Insider, Terrorist, FIS, Criminal | Intent | | | |
|---|---|---|---|---|
| | Knowledge of Asset | Need | Demonstrated Interest | Overall Intent Level |
| **Adversary 1** | Yes | Yes | Yes | High |
| **Adversary 2** | Yes | Yes | No | Medium |
| **Adversary 3** | Yes | No | No | Low |

*Figure 9: Intent Assessment Chart*

## 2.3 Determine the Capability of the Adversary

There are two distinct types of capability you will need to consider with respect to your adversary. The first is the capability to obtain, damage, or destroy the asset. The second is the adversary's capability to use the asset to achieve their objectives, once the asset is obtained. Thus, consider the following:

- Is the adversary aware that the asset exists?
- Does he know where assets are located?
- What do we know about the adversary's collection capabilities?
- What do we know about the adversary's methods of operation (e.g., suicide bombings, shootings, kidnapping, etc.)?

| Adversary<br>Insider, Terrorist, FIS, Criminal | Collection Capabilities | | | | |
|---|---|---|---|---|---|
| | HUMINT | SIGINT | IMINT | MASINT | OSINT |
| **Adversary 1** | High | High | Medium | Medium | High |
| **Adversary 2** | High | Medium | Low | Medium | High |
| **Adversary 3** | Medium | Medium | Low | Low | Medium |

*Figure 10: Capabilities Assessment Chart*

Figure 10 depicts a sample chart that can be used to document information collection capabilities of various adversaries. A rationale for each rating should be provided.

## 2.4 Determine Frequency of Threat-Related Incidents Based on Historical Data

A high frequency of threat-related incidents can indicate an increased likelihood that a similar incident may take place in the future, especially if capability and intent are high. However, an absence of previous incidents has little significance in predicting future incidents. In reviewing incident data, information pertaining to the following questions should be obtained and documented.

- What do you know about adversary's track record?
- How many suspected incidents?

- How many attempted incidents?
- How many successful incidents?

Figure 11 depicts a sample chart that can be used to document information pertaining to threat related incidents by various adversaries.

| Adversary | History | | |
|---|---|---|---|
| Insider Terrorist FIS, Criminal | Suspected Incidents | Attempted Incidents | Successful Incidents |
| Adversary 1 | 2 technical devices found | 2 attempted forced entries | Unknown |
| Adversary 2 | 5 alarm activations; adversary sighted in area | 2 attempted forced entries | Unknown |
| Adversary 3 | None | None | None |

*Figure 11: Sample Threat History Assessment Chart*

*Analyst's Note:* If there is a rich history of incidents, it may be useful to track events using a time/event flow chart to determine if there is an underlying pattern that could help predict future events. This technique is used frequently in the analysis of terrorist incidents.

## Putting It All Together

The chart shown in Figure 12 may be used to help identify and track information obtained during the steps outlined above.

*Analyst's Note:* If you determine that there is intent, but no capability or history on the part of the adversary, another consideration that must be addressed is the relation of your adversary to others who may have the capability. The key question here is,

**Threat Assessment Worksheet—FIS**

| Adversary | Intent | Capability | History | Rating |
|---|---|---|---|---|
| FIS—HUMINT | Yes<br>Anti-US stance<br>Known Tech Tgts<br>Known political tgts in UN, DC, Miami<br>Surrogates for others | Yes<br>Intell Os @ UN<br>Intell Os Miami Area<br>Spt infrastructure available<br>Tech penetration<br>SE | Yes<br>Last 5 years—<br>150 recruitment attempts<br>Bag Jobs<br>10 Arrests<br>20 Expelled<br>Dead drops ID | H / C |
| FIS—SIGINT | Yes<br>Defectors confirm | Yes<br>Phone intercept<br>Exchanges w/SVR | Yes<br>Exchanges w/SVR<br>Lourdes facility | M / H |
| FIS—IMINT | Yes<br>Defectors confirm | Yes-limited<br>Mostly hand-held<br>Commercial sat. | Yes<br>Agents observed<br>ComSat contracts | M / M |
| FIS—MASINT | Unknown<br>Assumed via HUMINT | Unknown<br>Assumed via HUMINT | Unknown | M / L |
| FIS—OSINT | Yes<br>Defectors confirm | Yes<br>HUMINT and UN Delegate collection observed | Yes<br>Analytical institute identified<br>Collection observed | L / C |

*Figure 12: Adversary Assessment Chart*

"Is the adversary allied with other entities, and what are their capabilities?" If a third party is identified, you will need to analyze the threat level using the same set of questions described above. If there is intent but no capability, one must consider that the adversary will make an attempt to achieve a capability. (Where there is a will, they will look for a way.) On the other hand, where there is a capability but no perceived intent, one must understand that intentions literally can change overnight, and some allowance should be factored into this possibility. Adversaries with a capability can use it when they want to.

## 2.5 Estimate the Degree of Threat Relative to Each Critical Asset and Undesirable Event

### Assessing Threats

The threat level is a relative rating based on best available information from the sources described above. To determine the relative degree of threat, rating criteria should be developed to allow for consistent rating of threat levels. Figure 13 is an example of a decision matrix with an explanation of each of the four rating categories.

Figure 14 provides an example of a tool which may be used to document the threat levels relative to a site's assets and related undesirable events and their impacts. The threat levels identified on the chart are based on threat information you obtained and documented earlier during Step 2. The product of this step is generally a site specific threat assessment report. * See Step 4 for a description of the relationship between linguistic and numerical scales.

### Threat Rating Criteria

**Critical** — Indicates that a definite threat exists against the assets and that the adversary has both the capability and intent to launch an attack, and that the subject or similar assets are targeted on a frequently recurring basis. (Numerical Rating Scale = .75 - 1.0)

**High** — Indicates that a credible threat exists against the assets based on our knowledge of the adversary's capability and intent to attack the assets and based on related incidents having taken place at similar facilities. (Numerical Rating Scale = .50 - .74)

**Medium** — Indicates that there is a potential threat to the assets based on the adversary's desire to compromise the assets and the possibility that the adversary could obtain the capability through a third party who has demonstrated the capability in related incidents. Indicates there is a significant capability with low or no current intent which may change under specified conditions. (Numerical Rating Scale = .25 - .49)

**Low** — Indicates little or no credible evidence of capability or intent, with no history of actual or planned threats against the assets. (Numerical Rating Scale = .0 - .24))

*Figure 13: Threat Rating Criteria*

*Analyst's Note:* The overall likelihood (probability) that any of these threats will place your organization's assets at risk is also dependent on the related vulnerability of the facility. It is important to understand that when you are estimating threat (T) ratings, you are looking specifically at the intent and capability of the adversary to target asset. Later in the ARM process this must be factored together with your vulnerability (V) rating determined in Step 3 to determine the likelihood of a successful attack. [Likelihood of a successful, unwanted event = T x V]

| Critical Asset | Undesirable Event/Impact | Threat Category | Threat Rating | # Rating |
|---|---|---|---|---|
| People | Motorcade attack → Assassination of VIP | Terrorist | H / C * | .97 |
| | Criminal activity → Kidnapping of employees | Terrorist | L / H | .50 |
| Information | Loss → Mission failure | FIS / Insider | H / H | .73 |
| | Unauth release → Disclose capability | Insider | M / M | .37 |
| Equipment | Theft → Loss of computers | Criminal | L / M | .30 |
| | Implant → Compromise information | FIS | H / H | .70 |
| Facilities | CBR → Denial of use | Terrorist | L / M | .25 |
| | Mail bomb → Destruction of property | Terrorist | H / H | .74 |
| Activities & Operations | Disrupt R&D → schedule setback | Militant | M / M | .37 |
| | Poor OPSEC → Operational disclosure | Insider / FIS | L | .12 |

*Note: See Step 4 for a description of linguistic and numerical scales
H/C = High/Critical, L/C = Low/Critical, etc.

*Figure 14: Threat Assessment Chart*

# Step 3: Identify & Characterize Vulnerabilities

Vulnerability assessments help us identify weaknesses that could be exploited to gain access to an asset. Determining a facility's physical and technical vulnerabilities involves not only an analysis of the facility's unique characteristics, but also of how the tenants function in and around the facility. During this step, shown in figure 15, risk analysts analyze critical assets as targets from an adversary's perspective. A vulnerability provides a pathway for creating an undesirable event and thus adverse impact(s). Using an adversary's perspective causes an analyst to develop attack scenarios which facilitate the identification of vulnerabilities.

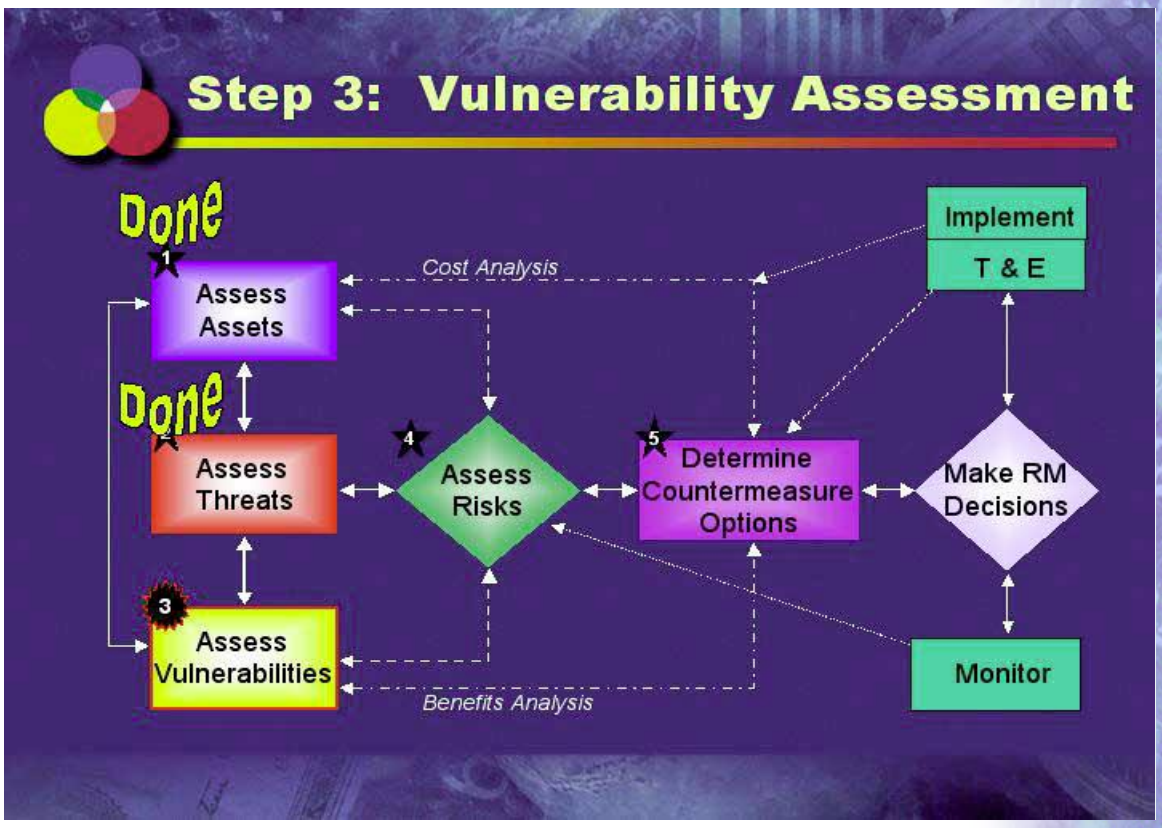



*Figure 15: Step 3 Flowchart*

**Vulnerability:** Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can result from, but are not limited to, the following: building characteristics, equipment properties, personal behavior, locations of people, equipment and buildings, or operational and personnel practices.

## 3.1 Identify Potential Vulnerabilities Related To Specific Assets And Undesirable Events

In Step 3, an analyst identifies the specific vulnerabilities associated with each asset, and the threat to that asset, using the information acquired during the previous steps. To determine where vulnerabilities exist, you must first determine the possible paths your adversaries might take. Next, determine what countermeasures are already in place and their relative degree of effectiveness in countering the assessed threats. Finally, identify and characterize the specific vulnerabilities that still exist given the current mix of countermeasures. As with the previous steps, an analyst should use a structured format to help track and document this information for future reference.

Within each of the asset categories listed, an analyst should identify and characterize specific, significant vulnerabilities related to the assets and the perceived threats against them. For example, in conducting a vulnerability assessment of a facility, all significant facility weaknesses that could be exploited to gain access to that facility should be separately identified, along with potential weaknesses of any countermeasures that may already be in place.

## Gathering Vulnerability Data

Sources for gathering vulnerability data include:

- Personnel who work at site
- Existing site surveys
- Engineering drawings and blueprints
- Maps
- Security planning documents, surveys and audits.
- Incident reports

Based on the protection of a specific asset, an analyst would determine which of these areas might be a path an adversary could use to exploit an asset. For each of the areas, one should list the countermeasures in place and determine existing weaknesses.

One of the most important aspects of this assessment is the analyst's understanding not only of the assets vulnerabilities, and the limitations of the existing countermeasures. Do the countermeasures really perform the job as they are intended to, or are assumptions being made about the capabilities of security devices with no hard evidence of their overall effectiveness? During this step of the process, it may be necessary to consult with experts who have technical skills.

In conducting a facility vulnerability assessment, examples of potential areas of vulnerability to consider are outlined below.

1. Physical Vulnerabilities:
   - Compound Perimeter Security (gates, stand-off distances, fences, walls, landscape, sewers, tunnels, parking area, alarms, guards, CCTV, etc.)
   - Compound Area (CCTV, motion detectors, lighting, etc.)
   - Building Perimeter (windows, doors, shipping docks, shielded enclosures, access control, alarms, etc.)
   - Building Interior (safes, locks, doors, vents, walls, ceilings, building construction history, opportunities for technical implants, etc.)

2. Technical Vulnerabilities:
   - Acoustic Equipment
   - Secure Phones
   - Tempest/TSCM
   - RF Equipment

3. Operational Vulnerabilities:
   - Guard Force
   - Personnel Procedures
   - OPSEC Issues — SOPS, Open Sources of Facility Information

Determining vulnerabilities also requires an understanding of adversary capabilities and their MOs for attacking a target. A question to ask is, "What typically do adversaries exploit?" Intercept of unsecured phone conversations? Faulty access control procedures? Employee character flaws? Collect trash? Poor trades craft? Understanding the types of vulnerabilities that adversary capabilities can exploit is another source for determining the vulnerabilities of an asset.

## 3.2 Identify Effectiveness of Existing Countermeasures

There may be conditions that inhibit the effectiveness of existing countermeasures and the proper operation of the overall security system. Some things to look for include:

- Obsolete or faulty equipment
- Poor procedures
- Poor training of end-user
- Human error
- Poor maintenance of equipment

Some questions to ask when assessing an existing system are:

- What type of protection do the existing countermeasures provide (deter, delay, detect, destroy, defend, defeat)?
- What type of undesirable events do they guard against (surreptitious entry, forced entry, technical implant, theft of classified material)?
- When are they effective — during which hours of the day/night and under what conditions?
- Where are they effective? What areas do they cover?
- What is the history of reported malfunctions (type, time, cause, pattern)?
- What is the correlation of countermeasure effectiveness to security incident reports that may indicate that the countermeasure was defeated?
- What is the history of countermeasure maintenance/upgrades?

Figure 16 provides a format that can be used for tracking countermeasures effectiveness against potential threats or undesirable events. Depending on the level of detail required, the matrix can either be used to link countermeasures to undesirable events, or it can be completed with a numerical rating indicating a relative level of effectiveness for each countermeasure. In Figure 16, a ten point scale was used with "1" being "extremely low" and "10" being "highly effective.' This matrix also shows if a countermeasure has some degree of effectiveness against multiple undesirable events.

*Figure 16: Existing Counterneasures Effectiveness*

| Existing Countermeasures *Effectiveness Rating* | Undesirable Events: Surreptitious Entry (1-10) | Kidnapping/ Assassination (1-10) | Documents Stolen/Mishandled (1-10) | Terrorist Attack Bombing (1-10) |
|---|---|---|---|---|
| Doors, locks, bars | 7 | 7 | 4 | 2 |
| Alarm/sensors | 5 | 8 | 7 | 2 |
| Contractor guards | 7 | 8 | 7 | 2 |
| Spec. Police Officers | 9 | 9 | 6 | 2 |
| Marine Guards | 9 | 9 | 8 | 3 |
| Vary travel route | - | 5 | 8 | - |
| Relocate Gov. Official | - | 8 | 6 | - |
| Residence locks, bars | - | 4 | - | - |
| Disguise | - | 8 | - | - |
| Bullet-proof car | - | 5 | - | - |
| Residence CCTV | - | 4 | - | - |
| Security awareness | 5 | 7 | 7 | 9 |
| Strict media controls | - | - | 6 | - |
| System audit trail | - | - | 6 | - |
| Passwords | - | - | 6 | - |
| Defense driving training | - | 5 | - | - |
| Vehicle checks | - | 5 | - | 7 |
| Emerg. Procedures | - | 5 | - | 4 |
| Metal detector | - | 5 | - | 5 |
| Fences/barriers | - | - | - | 6 |

Vulnerability data should be linked directly to specific undesirable events. Physical and operational vulnerabilities should be listed. Figure 17 provides a format for linking vulnerabilities to undesirable events. Note how some vulnerabilities provide pathways for multiple undesirable events. This information is required in order to assess vulnerability levels associated with each potential undesirable event. It will help in guiding your selection of countermeasures once the risk areas have been prioritized in Step 4.

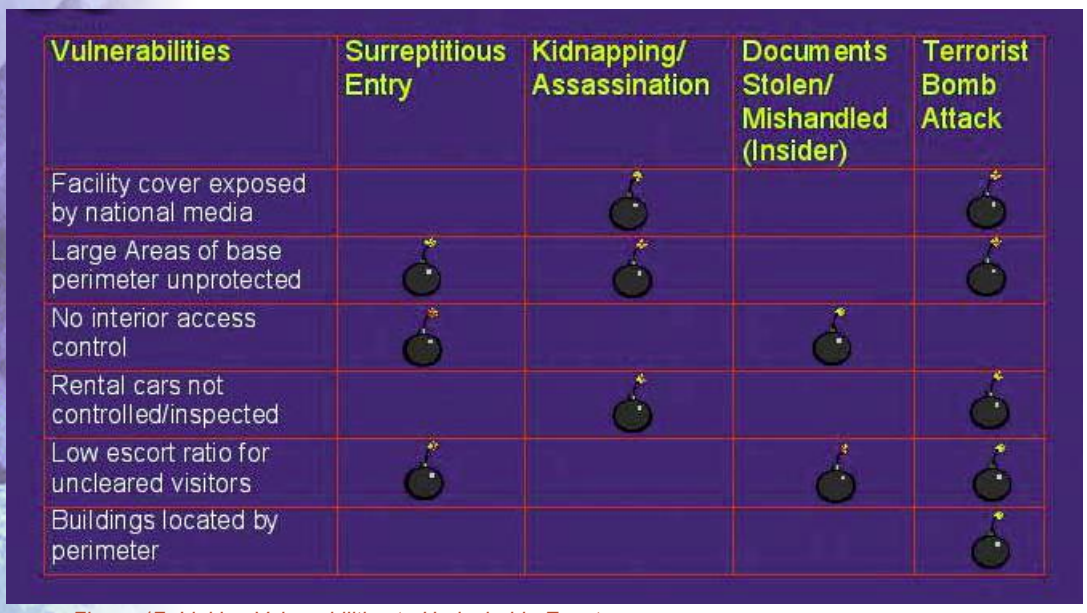



*Figure 17: Linking Vulnerabilities to Undesirable Events*

## 3.3 Determine Vulnerability Level

The likelihood (probability) that a targeted vulnerability will be successfully exploited is a function of the number and effectiveness of the security countermeasures put into place. If few, ineffective, or no countermeasures are put in place, the likelihood that an adversary will be successful is very high. As redundant layers of effective security countermeasures are applied (defense in depth), the likelihood of successful exploitation drops, since the vulnerabilities and consequently the risk are reduced or eliminated.

Criteria used to determine vulnerability will vary depending upon the type of asset, its value, and its location. Below are three questions that may be used to determine the vulnerability levels of an asset.

1. Is the asset made vulnerable by a single weakness or multiple weaknesses in the security protective system?
2. Does the nature of the vulnerability make it difficult to exploit?
3. Is the vulnerability of the asset lessened by multiple, effective layers of security countermeasures?

To answer these three questions, an analyst must collect data from a variety of sources to identify the vulnerabilities. After answering yes or no to the three questions above, a decision matrix such as shown in Figure 18 may be used as a guide in determining the vulnerability level.

As in previous steps, rating criteria must be developed to ensure consistency. Specifically, an analyst must establish a linguistic and/or numerical scale and define what is meant by the different increments of that scale as illustrated by the Vulnerability Rating Criteria in Figure 18.

The risk analyst completes Step 3 by using the data derived from the vulnerability analysis to continue building a risk assessment chart. As shown by Figure 19, vulnerability ratings are expressed for each undesirable event and its associated impact.

*See Step 4 for a description of the relationship between linguistic and numerical scales.

*Analyst's Note:*
Soft targets can enhance the adversary's intent. The vulnerabilities themselves can also influence the likelihood that the undesirable event will occur and succeed. If few vulnerabilities exist, or if the nature of the vulnerabilities makes them difficult to exploit, it is less likely that they will be exploited. If the vulnerabilities have not been identified or protected, or if they are easy to exploit, the likelihood of the event occurring increases.

With the completion of Step 3, all of the elements for determining relative risk (R) are available to the analyst — Impact (I), Threat (T) and Vulnerability (V) have been identified and rated.

## Vulnerability Rating Criteria

**Critical** — Indicates that there are few effective countermeasures currently in place and principal known adversaries would be capable of exploiting the asset.
(Numerical Rating Scale = .75 - 1.0)

**High** — Indicates that although there are some countermeasures in place, there are still multiple weaknesses through which many adversaries would be capable of exploiting the asset.
(Numerical Rating Scale = .50 - .74)

**Medium** — Indicates that there are effective countermeasures in place, however at least one weakness does exist which some known adversaries would be capable of exploiting.
(Numerical Rating Scale = .25 - .49)

**Low** — Indicates that multiple layers of effective countermeasures exist and few or no known adversaries would be capable of exploiting the asset.
(Numerical Rating Scale = .01 - .24)

*Figure 18 Rating Criteria*

| Critical Asset | Undesirable Event/Impact | Threat Rating | # Rating | Vuln Rating | # Rating |
|---|---|---|---|---|---|
| People | Motorcade attack → Assassinate VIP | H / C | .97 | L / H | .50 |
| | Criminal activity → Kidnap employee | L / H | .50 | L / M | .25 |
| Information | Loss → Mission failure | H / H | .73 | H / M | .49 |
| | Unauth release → Disclose capability | M / M | .37 | M / M | .37 |
| Equipment | Theft → Loss of computers | L / M | .30 | H / M | .45 |
| | Implant → Compromise information | H / H | .70 | L | .12 |
| Facilities | CBR → Denial of use | L / M | .25 | H / H | .74 |
| | Bomb → Destruction of property | H / H | .74 | L / M | .25 |
| Activities & Operations | Disrupt R&D → Schedule setback | M / M | .37 | L | .24 |
| | Poor OPSEC → Operational disclosure | L | .12 | H / M | .49 |

*Note: See Step 4 for a description of linguistic and numerical scales
H/C = High/Critical, L/C = Low/Critical, etc.

*Figure 19: Vulnerability Assessment Chart*

# Step 4: Assess Risks & Determine Priorities For Asset Protection

During this step, an analyst estimates the likelihood (probability) that a specific undesirable event will occur given current conditions and/or "what if" scenarios. The assessment is based on an integration of the data collected on assets (Steps 1,2, and3), see Figure 19. threats and vulnerabilities.


*Figure 20: Step 4 Flowchart*

## 4.1 Estimate the Degree of Impact Relative to Each Critical Asset

During this step you should review your impact rating from Step 1, taking into consideration the information obtained in Steps 2 and 3. Solicit other judgments and make necessary revisions to the analysis.

## 4.2 Estimate the Likelihood of Attack by a Potential Threat or Adversary

During this step you will review your threat rating from Step 2, taking into consideration the information obtained in Steps 1 and 3. Solicit other judgments and make necessary revisions to the analysis.

## 4.3 Estimate the Likelihood that a Specific Vulnerability will be Exploited

During this step you will review your impact rating from Step 3, taking into consideration the information obtained in Steps 1 and 2. State other judgments and make necessary revisions to the analysis.

**Risk:** Risk is the potential for damage to or loss of an asset. The level of risk is a combination of two factors:
1. The value placed on that asset by its owner and the consequence, impact, or adverse effect of loss or damage to that asset (the I), and
2. The likelihood (probability) that a specific vulnerability (V) will be exploited by a particular threat (T). (See Figure 21.)

**Risk Assessment** (R) is the process of determining the likelihood (probability) of an adversary (T) successfully exploiting a vulnerability (V) and the resulting degree of damage or impact (I) on an asset. A risk assessment provides the basis for rank ordering risks and thus establishing priorities for the application of countermeasures. Thus the formula R = I x (T x V) is used.

## 4.4 Determine the Relative Degree of Risk

The chart in Figure 22 provides a means of identifying and tracking the individual judgments made to determine the overall risk level. When the threat (T) and vulnerability (V) levels are considered together, an analyst can estimate the probability or likelihood of occurrence of the

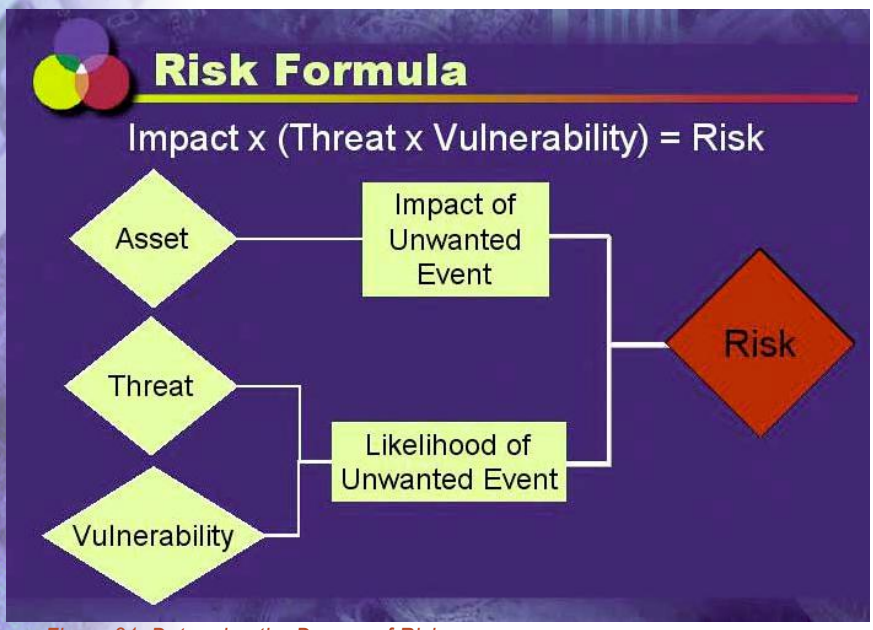



*Figure 21: Determine the Degree of Risk*

undesirable event. Probability of occurrence of the undesirable event (T x V) and expected Impact (I) are considered together in the estimate of the risk level. Using a numerical rating system (see Figure 23), the overall risk can be computed by using the following formula:

Risk = Impact x (Threat x Vulnerability)

Why multiply? Using multiplication in the formula is based on the premise that all three elements (I and T and V) must be present to have risk (R). Thus, if there is no threat (T), there is no risk (R). Likewise, if there is no vulnerability (V) for the threat (T) to exploit, there is no risk (R). Furthermore, even if there is a threat (T) and a vulnerability (V) to exploit but there is no consequence or impact (I) of that exploitation, there is no risk (R). Thus, to get a "no risk" outcome in the formula (i.e., R = 0 [zero]) when I and/or T and/or V are zero, requires using multiplication.

An undesirable event has an "expected impact (I)," while threat (T) and vulnerability (V) are considered together to determine the "probability" of the undesirable event occurring. The risk equation takes into account both the likelihood and magnitude of the undesirable event.

| Critical Assets | Potential Undesirable Events | Asset Rating | # Rating | Threat Rating | # Rating | Vuln. Rating | # Rating | Risk Rating |
|---|---|---|---|---|---|---|---|---|
| People | Motorcade Attack→ Assassinate VIP | H/C | 97 | H/C | .97 | L / H | .50 | H/H (47) |
| | Criminal Act→Kidnap employee | L/C | 50 | L/H | .50 | L / M | .25 | M/M (6) |
| Information | Loss → Mission failure | H/C | 97 | H/H | .73 | H / M | .49 | H/H (35) |
| | Unauth release → Discl Capa | H/M | 13 | M/M | .37 | M / M | .37 | L (2) |
| Equipment | Theft →Loss of computers | L/M | 3 | L/M | .30 | H / M | .45 | L (1) |
| | Implant → Compromised info | H/H | 48 | H/H | .70 | L | .12 | L/M (4) |
| Facilities | RBC → Denial of use | M/H | 25 | L/M | .25 | H / H | .74 | M/M (5) |
| | Mail Bomb → Destroy property | L | 2 | H/H | .74 | L / M | .25 | L (1) |
| Activities & Operations | Disrupt R&D → Sched setback | M/M | 5 | M/M | .37 | L | .24 | L (1) |
| | Poor OPSEC → Op disclosure | L/H | 15 | L | .12 | H / M | .49 | L (1) |

*Figure 22: Assess Risk and Determine Priorities*

Where vulnerabilities are great and the threat is evident, the risk of exploitation is greater. Therefore, a higher priority for protection must be considered. Where the vulnerability is slight and/or the adversary has little capability to exploit vulnerabilities, now or in the future, the risk is lower and the priority for new countermeasures is lower. The areas of greatest risk that are identified by the risk assessment will serve as the basis for deciding where to focus countermeasures and what countermeasures to apply.

The scale used in this guide is linguistic and numerical and this relationship is shown in Figure 22. The Impact (I) and Risk (R) portion of the scale are exponential to describe the ever-increasing severity of impact (I) and hence risk (R) as you move up the scale from low to critical. The ranges established for threat (T) and vulnerability (V) are shown as probabilities to express the likelihood of a threat's success in creating an unwanted event.

The ratings used (linguistic and/or numerical) for each step of the risk assessment process rest on establishing definitions for the terms and for the ranges of numbers used to establish a scale. The analyst must make the definitions as precise as possible, describing, as an example, what is meant by "Critical, High, Medium, and Low" and the numerical range assigned to each of these terms (for example, the numerical range for "Critical" might be 50 to 100 on a 100 point scale). If more granularity is required you can establish three levels within each of the linguistic categories as shown in the chart below. To maintain consistency and objectivity, definitions should be read each time prior to assigning a rating.

Impact or Risk

| | Low | Medium | High | Critical |
|---|---|---|---|---|
| Range | 1-3 | 4-13 | 14-49 | 50-100 |
| Mid-point | 2 | 5 | 25 | 71 |

Threat or Vulnerability

| | Low | Medium | High | Critical |
|---|---|---|---|---|
| Range | .01-.24 | .25-.49 | .50-.74 | .75-1.00 |
| Mid-point | .12 | .37 | .62 | .87 |

*Figure 23: Relating Linguistic & Numerical Scales*

## 4.5 Identify Unacceptable Risks and Determine Risk Mitigation Priorities

The final step within the risk assessment process is to determine your security protection priorities. All of the previous steps have been done to help make a rational assessment of risks and which are most serious and to rank order them relative to each other.

### What Is an Acceptable Level of Risk?

Who Decides? The acceptable level of risk for an asset cannot be determined by a formula. It may vary with time, circumstances, and management's attitude toward risk in the organizational environment. It is the sponsors or owners of the asset who must ultimately decide what constitutes an acceptable level of risk for their assets. The risk ratings shown in figure 22 can help the decision maker determine what may or may not be acceptable. For example, the decision maker may find that low and medium risk ratings are acceptable while critical and high risks are not acceptable thus requiring the application of additional countermeasures.

H/C, M/C, L/C } CRITICAL

H/M, M/M, L/M } MEDIUM

H/H, M/H, L/H } HIGH

H/L, M/L, L/L } LOW*

*Linguistic Categories*

# Step 5: Identify Countermeasures, Costs, & Options

Based on the information obtained and analyzed in the previous steps, you can now identify countermeasures that reduce the vulnerabilities linked to your unacceptable risks. You could choose to employ a single countermeasure,or several countermeasures used in combination, to lower risk for each event. Two or more countermeasures may work together in a compensating fashion to guard against a vulnerability that neither would provide adequate protection for individually. Figure 24 provides an overview of where we are in the ARM process.

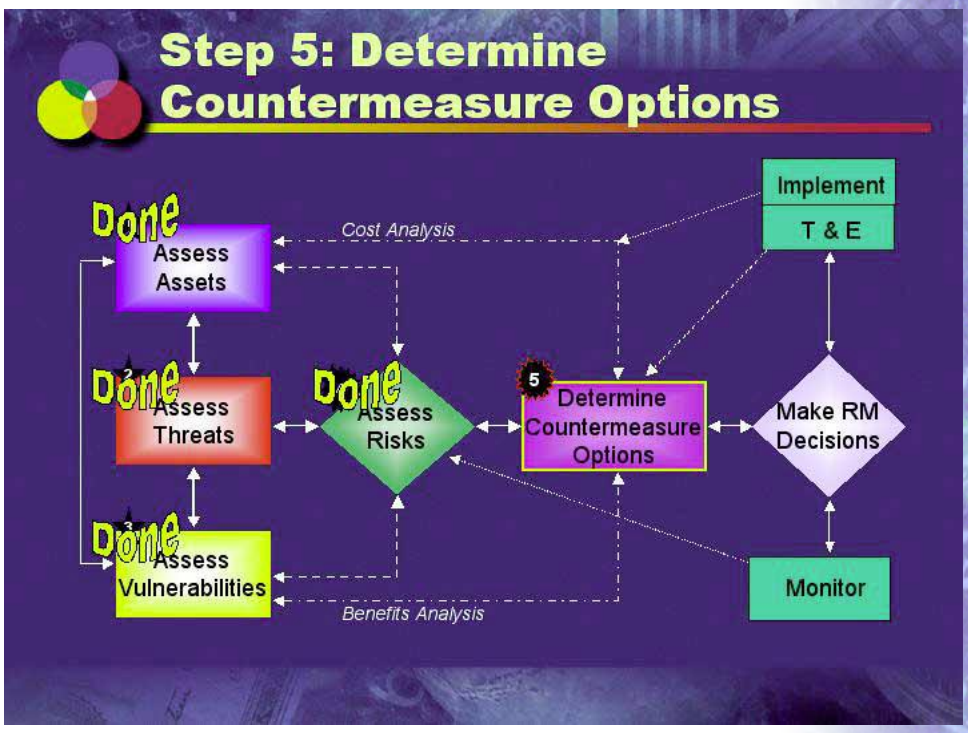



*Figure 24: Step 5 Flowchart*

## 5.1 Identify Potential Countermeasures to Reduce Vulnerabilities

During Step 5, you will consider the possible protection solutions for specific undesirable events with a goal of minimum cost and maximum risk reduction.

Countermeasures generally fit into one of the following three categories: (1) procedures, (2) equipment, and (3) manpower. Examples of countermeasures are found in figure 25.

**Countermeasure:** A countermeasure is an action taken or a physical entity used principally to reduce or eliminate one or more vulnerabilities. Countermeasures may also affect the threat (intent and/or capability) as well as an assets value. The cost of a possible countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

**Cost-Benefit Analysis:** A cost-benefit analysis is the part of the management decision-making process in which the costs and benefits of each alternative are compared and the most appropriate alternative is selected. Costs include not only the cost of tangible materials, but also the on-going operational costs associated with countermeasure implementation. Benefits are expressed in terms of the amount of risk reduction based on the overall effectiveness of the countermeasures with respect to the assessed vulnerabilities.

## 5.2 Identify the Function and Effectiveness of Each Countermeasure

During this step, an analyst should consider the following questions: How does this countermeasure mitigate risk? Does this countermeasure deter, detect, delay, deny/defend or defeat/ destroy the threat? Figure 25 provides a matrix which assists in making these determinations.

To what degree does this countermeasure mitigate risk? A quantitative rating may be used, as shown in figure 26, or a linguistic rating such as high, medium, or low. This matrix will help track judgments related to the relative level of risk reduction and benefit gained with each countermeasure.

| Procedures | Equipment | Manpower |
|---|---|---|
| OPSEC procedures | Locking mechanism | Contractor Guards |
| Asset Transfer | Window bars | SPOs |
| Training | Doors | Local Guards |
| Awareness programs | Fences | Marine Guards |
| Legal prosecution | Alarms/sensors | |
| Polygraph | Hardware/software | |
| Security investigations | Badges | |
| Disclosure statements | Lighting | |
| Personnel transfer | Tempest devices | |
| Contingency planning | Paper shredder | |
| Cover stories | Weapons | |
| Two Person Rules | Closed circuit TV | |
| Passwords | Safe haven | |
| Periodic Searches | Vault | |

*Figure 25: Example Countermeasures*

## 5.3 Identify the Benefits of the Countermeasures

To identify countermeasure options packages, one can use a format similar to the one presented in Figure 26. Countermeasure benefits can be defined in terms of the level of risk reduction that they provide. A countermeasure option package can be defined as "grouping of security countermeasures that work together as a security system to guard against the significant risks identified during the risk assessment phase." To determine the most effective sets of countermeasures for each of the undesirable events identified, the effect that each countermeasure option will have on the existing risk level must be determined. This can be accomplished by answering the questions about vulnerability again (Step 3) and also by considering if the countermeasure options also will have an affect on the threat (intent and/or capability) or on the asset (a lessening of the impact). The analysis of countermeasure functions (Figure 26) and countermeasure effectiveness (Figure 27) supports your risk reduction analyses. Following this procedure a determination is made of the new level of risk using the matrix shown previously in Figure 22 by establishing new values for V (and/or T, and/or I ) as a result of the proposed countermeasure. Figure 28 shows this linkage of countermeasure options to vulnerabilities and undesirable events. Appendix C outlines a step by step process for developing countermeasure option packages.

| | Countermeasure Functions | | | | |
|---|---|---|---|---|---|
| Countermeasure (Effectiveness 1=Low; 10=Hi) | Deter | Detect | Delay | Deny/ Defend | Defeat/ Destroy |
| Doors, locks, bars | 6 | - | 4 | 4 | - |
| Alarm/sensor (visible) | 7 | 8 | 8 | - | - |
| Contract guards | 7 | 7 | 7 | 7 | 7 |
| Vary travel route | 5 | - | - | - | - |
| Relocate VIP | 5 | - | - | 5 | - |
| CCTV (visible) | 7 | 7 | 2 | - | - |
| Bullet proof car | 7 | - | 7 | 7 | - |
| Security awareness | 7 | 2 | 3 | 5 | 5 |
| Metal detectors | 7 | 7 | - | - | - |
| Ready force | 9 | - | 2 | 9 | 9 |

*Figure 26: Countermeasures Function Matrix - VIP Protection*

Certain countermeasures may appear several times in a matrix. If one of these countermeasures is selected, it could mitigate the risk of several undesirable events.

## 5.4 Identify the Cost of the Countermeasures

During this step, an analyst considers the cost of tangible materials, and also the on-going operational costs associated with countermeasure implementation. An analyst must keep in mind that using specified procedures are usually the least expensive type of security countermeasures. Hardware is general-

ly more expensive than procedures, and manpower costs are usually the most expensive form of countermeasure. Every countermeasure has a cost associated with it that can be measured in terms of dollars, inconvenience, time, or personnel. In order to select the most appropriate countermeasure option, the cost associated with each countermeasure must be determined. Figure 29 provides a format for identifying countermeasures and their costs.

| New Countermeasures *Effectiveness Rating* | Undesirable Events: Surreptitious Entry | Kidnapping/ Assassination (1-10) | Documents Stolen/Mishandled (1-10) | Terrorist Attack Bombing (1-10) |
|---|---|---|---|---|
| Doors, locks, bars | 7 | 7 | 7 | 2 |
| Alarm/sensors | 5 | 8 | 5 | 2 |
| Contractor guards | 7 | 8 | 7 | 2 |
| Spec. Police Officers | 9 | 9 | 9 | 2 |
| Marine Guards | 9 | 9 | 9 | 3 |
| Vary travel route | - | 5 | - | - |
| Relocate Gov. Official | - | 8 | - | - |
| Residence locks, bars | - | 4 | - | - |
| Disguise | - | 8 | - | - |
| Bullet-proof car | - | 5 | - | - |
| Residence CCTV | - | 4 | - | - |
| Security awareness | 5 | 7 | 7 | 9 |
| Strict media controls | - | - | 6 | - |
| System audit trail | - | - | 6 | - |
| Passwords | - | - | 6 | - |
| Defense driving training | - | 5 | - | - |
| Vehicle checks | - | 5 | - | 7 |
| Emerg. Procedures | - | 5 | 7 | 4 |
| Metal detector | - | 5 | - | 5 |
| Fences/barriers | - | - | 5 | 6 |

*Figure 27: Countermeasures Effectiveness Matrix*

When determining the dollar cost of a countermeasure, include the purchase price as well as the life-cycle maintenance costs. This may include installation, preventative maintenance, repair, warranty, replacement and disposal costs. The life expectancy of the countermeasure should be considered when determining cost. Dollar cost may also include the salaries of staff or contractors to implement, maintain, monitor, or train others to use the countermeasure.

When determining the cost of a countermeasure in terms of inconvenience, consider whether the inconvenience caused is offset by the measure of risk reduction gained. If a countermeasure is inconvenient, people will find a way to bypass it. It is possible that through redesign the procedure, the same or greater level of risk reduction can be achieved with far less inconvenience.

| Undesirable Event | Existing Risk Level | Related Vulnerabilities | Countermeasure Options | Reduced Risk Level |
|---|---|---|---|---|
| Stand off Technical attack on automated Information systems | High/High | Compromising emanation w/in range of adversary | Replace w/ TEMPEST equip.<br>Use RF Shielding<br>Move equip. out of range | Low<br>Low<br>Low |
| Terrorist Attack on Government Official | High/Med | Symbolic target<br>Personnel unaware of threat<br>Recent media exposure | OPSEC procedures<br>Security briefing<br>Surveillance | Low/Med<br>Low/Med<br>High/Med |

*Figure 28: Linking Countermeasure Options to Vulnerabilities and Undesirable Events*

When determining the cost of a countermeasure in terms of time, include the time to implement or oversee the countermeasure and the time to prepare for implementation, as well as any time required for follow-up and evaluation. When determining the cost of a countermeasure in terms of the personnel required to use it, consider the number of staff needed to use the counter measure as well as the skills, knowledge, and abilities of the personnel involved. Additionally, staff training needs/ costs should be considered.

| Undesirable Events | Procedures | Equipment | Manpower |
|---|---|---|---|
| Surreptitious Entry | Procedures to secure facility after hours<br>Cost: $5,000<br>Cost: moderately inconvenient<br>Cost: $20,000 | Doors, locks, bar<br><br>Cost: $100,000<br>Alarm/sensor system<br>Cost: $200,000<br>Marine Guards<br>Cost: $250,000 | Contractor guards<br><br>SPOs |
| Kidnapping/ Assassination | Vary travel route to work<br>Cost: minimal inconvenience<br>Relocate Govt. official to compound<br>Cost: $10,000<br>Cost: $40,000<br>Residential CCTV<br>Cost: $17,000 | Doors, locks, bar<br>Cost: $5,000<br>Alarm/sensor system<br>Cost: $30,000<br>Bullet-proof car | Contractor guards<br>Cost: $100,000<br>SPOs<br>Cost: $250,000 |
| Documents Stolen/Mishandled | Security Awareness Briefing<br>Cost: negligible<br>Strict magnetic media control procedures<br>Cost: moderately inconvenient | System audit trail<br>Cost: $125,000<br>Passwords<br>Cost: $50,000 | N/A |
| Terrorist Bomb attack | Defensive driving training<br>Cost: $80,000<br>Vehicle checks<br><br>Cost: $200,000<br>Emergency procedures<br>Cost: $15,000<br>Fences/barriers<br>Cost: $90,000 | Doors, locks, bars<br>Cost: $5,000<br>Alarm/sensor system<br>Cost: $200,000<br><br>Metal detectors<br>Cost: $20,000 | Contractor guards<br>Cost: $100,000<br>SPOs<br>Cost: $30,000<br><br>Marine guards<br>Cost: $250,000 |

*Figure 29: Potential Countermeasures and Costs*

The general principle to follow when analyzing countermeasures is to select the least expensive countermeasure that will and reduce the risk to an acceptable level. However, since a countermeasure may protect against more than one vulnerability, and since compensating countermeasures are used in a complementary manner to form a security system, it is important to determine the cost of the various optional countermeasure groupings. A particular grouping may be less expensive than the sum of the costs of countermeasures for each significant unwanted event identified and provide adequate protection at an overall lower cost because of the mutual support across multiple undesirable events of the countermeasure grouping. After the cost of each optional countermeasure grouping is determined, the cost differences and the marginal benefits of each option can be compared.

### Getting Cost Data

Finding reliable cost data for countermeasures may not be easy but it is required. The analyst must provide decision makers at least a reasonable estimate of what implementing the various countermeasures will cost in terms of dollars, time, maintenance, life-cycle, training, personnel, and so forth. One time costs as well as recurring costs should be identified. The first place to start in gathering cost-data is a local procurement office. This office may have recently contracted for countermeasure equipment (e.g., fences, barriers, alarms/sensors) or services (e.g., contract guards). As a minimum, they can offer advice on how to collect such information from vendors without implying a commitment to buy. Various professional security organizations provide both on-line and hard-copy "buyers" guides that are organized into various categories of goods and services. The American Society for Industrial Security annually prepares a very comprehensive guide. The GSA also has limited listings of security and safety vendors and costs. Another source is the Internet. Simon.net lists in excess of 5,000 vendors and provides hotlinks to their sites where available.

## 5.5 Analyze the Cost Compared to the Benefit of Each Option

Based upon the results of the risk assessment, an analyst will determine the various countermeasure options available to mitigate the risk, thereby reducing it to an acceptable or conditionally acceptable level. Two key questions which need to be asked include:

1. How does the impact on asset value of an undesirable event compare to the proposed cost of protection?
2. Which options provide the best protection at the lowest cost?

There are no simple answers. The cost of protective measures typically should not exceed a reasonable percentage of the total undesirable event's impact value on the assets requiring protection. However, there is no one "reasonable" percentage. The asset owners or program managers responsible for these assets must balance the benefits of risk reduction against the cost of reducing risk.

Factors which influence countermeasure decisions include:

- Value of the asset — What impact does it have if lost or damaged?
- Current exposure to loss/harm — How vulnerable is the asset?
- Availability of protective measures — What is the state-of-the-art and effectiveness?
- Availability of funds — What resources are available compared to asset value?
- Mandatory security requirements — What is mandated by law or regulation?

## 5.6 Prioritize Countermeasure Options That Address Risks

Notice that Countermeasure Option 1 — Maximum Protection, presented in Figure 30, reduces the overall average risk level for these four unwanted events from high/high to low at a cost of $1,065,000. Countermeasure Option 2 —Recommended Option, presented in figure 31, reduces the overall average risk level from high/high to medium/medium at a cost of $230,000. Countermeasure Option 3 — Least Expensive Option, presented in figure 32, only costs $35,000 but does not reduce the overall average risk level. Option 2 would most likely be the preferred option because it offers the greatest risk reduction and best return on investment.

| Undesirable Events | Countermeasures | Risk Level Reduced From/To | Cost |
|---|---|---|---|
| Surreptitious Entry | Guards<br>Doors, locks, bars<br>Alarm/sensor system | LOW/HIGH to LOW | $250,000<br>$5,000<br>$20,000 |
| Terrorist bomb attack | Defensive driving training<br>Vehicle checks<br>Emergency procedures<br>Metal detectors<br>Fences/barriers | HIGH/CRITICAL to LOW | $80,000<br>$200,000<br>$15,000<br>$20,000<br>$90,000 |
| Documents Stolen/ Mishandled | System audit trail<br>Passwords<br>Security awareness briefing | LOW/MEDIUM to LOW | $125,000<br>$50,000<br>Minimal |
| Kidnapping/ Assassination | Vary travel route to work<br>Bullet-proof car<br>SPOs at Gov. Off. Residence | MEDIUM/MEDIUM to LOW | (inconvenient)<br>$40,000<br>$170,000 |
| | OVERALL RISK<br>TOTAL COST | HIGH/HIGH to LOW | $1,065,000 |

*Figure 30: Countermeasure Option 1 (Maximum Protection)*

| Undesirable Events | Countermeasures | Risk Level Reduced From/To | Cost |
|---|---|---|---|
| Surreptitious Entry | Contract Guards<br>Doors, locks, bars, alarms/sensors | LOW/HIGH to LOW/MEDIUM | $100,000<br>$5,000<br>$20,000 |
| Terrorist bomb attack | Emergency procedures<br>Fences/barriers | HIGH/CRITICAL to HIGH/MEDIUM | $15,000<br>$90,000 |
| Documents Stolen/ Mishandled | N/A | LOW/MEDIUM to N/A | N/A |
| Kidnapping/ Assassination | N/A | MEDIUM/MEDIUM to N/A | N/A |
| | **OVERALL RISK<br>TOTAL COST** | **HIGH/HIGH to MEDIUM/MEDIUM** | **$230,000** |

*Figure 31: Countermeasure Option 2 (Recommended Option)*

Once several options are determined, their advantages and disadvantages should be presented to the customer. One of the options should be recommended and the rationale clearly spelled out. The customer makes the final decision about countermeasures employed and assumes the risk(s) present in that option. As noted several times, the goal of Step 5 is to provide least cost/maximum benefit options to a decision maker.

| Undesirable Events | Countermeasures From/To | Risk Level Reduced | Cost |
|---|---|---|---|
| Surreptitious Entry | | HIGH to N/A | N/A |
| Documents stolen/ Mishandled | | LOW/MEDIUM to L/M | N/A |
| Kidnapping/ Assassination | | MEDIUM/MEDIUM to N/A | N/A |
| Terrorist bomb attack | Emergency procedure<br>Metal Detectors | HIGH/CRITICAL to<br>MEDIUM/CRITICAL | $15,000<br>$20,000 |
| | **OVERALL RISK TOTAL COST** | **HIGH/HIGH to HIGH** | **$35,000** |

*Figure 32: Countermeasure Option 3 (Least Expensive Option)*

# Applying the ARM Process to Customer Requirements

Before applying the systems approach outlined in this guide to a particular situation or customer requirement, it is important to understand the nature of the task an analyst is about to undertake. Following the preliminary steps outlined below will help determine if the analytical risk management methodology is appropriate to the task, and to what extent the methodology should be applied in conducting the analysis. Most important, it will help develop a common understanding of the nature of the analysis to be conducted with the security team members and the customer. The key steps for doing this include:

- Clarify the purpose of the task
- Scope the task/problem
- Determine constraints
- Identify approach and end product
- Validate requirement with the customer.

## 1. Clarify the Purpose of the Analysis

What decision(s) will be made based on the analysis? State the purpose of the decision(s) to be made. What is the ultimate goal, or result to be achieved from the decision? Who asked the question? Who is the customer? Is there more than one customer and how do they relate to each other? Who is the decision maker? Is there more than one and how do they relate to each other? What do they want to know? Why do they need your support?

## 2. Scope the Task/Problem

State the scope of the problem or task. What will your analysis include and what will not be included in the analysis? What level of detail is required to back up the analytical findings? How long will the information base of the analysis be valid? Will other information be supplied to the decision maker from different sources and of what type?

## 3. Determine Constraints/Assumptions

List the constraints and assumptions related to conducting the analysis. What access does the analyst have to the best sources of information? Where are anticipated problems in obtaining the information needed? What is the customer's influence? Are there politically correct and incorrect answers? Are there multiple customers with conflicting interests? What are the driving political, economic, or legal constraints that could have an impact on the ability to successfully complete the task? What are the resource constraints? Does the customer have the authority and resources to implement changes once the analysis is provided? Is it appropriate to conduct the analysis at this time?

## 4. Identify the Analytical Approach and the End Product

Identify the type of product requested. What type of assessment and product do they actually need to answer their question(s)? What specific information is needed to conduct the assessment? What sources are available? Customer products that are used to document elements of the risk management process may include:

- Asset assessment (Assesses critical assets - people, information, equipment, facilities, activities/operations)
- Impact assessment (Assesses potential undesirable events and their impacts)
- Threat assessment (Assesses threats and adversary motives/intentions, capabilities and history)
- Vulnerability assessment (Assesses weaknesses in the security of critical assets)
- Risk assessment (Assesses overall risk based on identified assets and the consequences of undesirable events, threats, and vulnerabilities)
- Countermeasures cost/benefit analysis (Analyzes the cost of countermeasures compared to an assets impact loss value and the benefit of countermeasures in terms of overall risk reduction capability)
- Risk management report (Provides overall risk assessment and recommends CM options)

Assessments can take place at various levels to include the following:

- Zero-based assessment (Assesses requirements assuming no security plan exists)
- Baseline assessment (Assesses effectiveness of existing security plan)
- Comparative analysis (Analyzes requirements based on deviations from standard/baseline)

*Figure 32: Sample Task Statement*

### Sample Task Statement

The Risk Assessment Team will conduct a series of site visits and interviews with a select group of personnel at the XYZ site. The purpose of the visits/interviews is to identify critical assets at the site and the potential undesirable events that may adversely affect those assets together with their estimated impacts. Additionally, the team will develop relevant threat data necessary to determine those adversaries having the motivation/intent to target the identified critical assets as well as identify the sites vulnerabilities the threat might exploit to achieve their objectives. Interviewees will be carefully chosen so that the information obtained will include the concerns and opinions of employees of various positions and grades. Throughout these interviews, a consistent series of topics and questions will be covered with each interviewee in order to determine site-specific information on critical assets, threats, and vulnerabilities.

The individuals to be interviewed as a minimum will include: Chief of Facility; Chief, Administrative Services; Chief, Operational Training; Chief, Security; and Deputy Chief, Security, Captain, Special Protective Service. Information related to the site's current security posture and the specific countermeasures in place there will be derived primarily through interviews with site security personnel and the recent zero-based review.

In addition to information provided by site personnel, threat data will be obtained from a variety of outside sources and coordinated by assigned matrix counter-intelligence support personnel. These sources include the National Counterintelligence Center (NACIC), FBI, Counter Terrorist Center (CTC), and Military Police.

This assessment will also be based on Headquarters' information contained in recent threat assessments conducted for other domestic facilities in the Washington area. A survey of open source data will be conducted using the Lexis/Nexis database to determine the degree of exposure the covert site has had.

The Risk Assessment Team will provide the site manager with a Risk Management Report outlining findings, conclusions, and recommendations for the application of countermeasures designed to protect critical assets. A cost/benefit approach will be used by the team as a basis for such recommendations. The report will be delivered 30 days after task initiation.

- Justification statement (Provides rationale for a decision already made)

## 5. Validate the Customer Requirement with the Customer

Confirm the customer's request with a documented task statement similar to the example shown in figure 32. What will the analyst provide as a product? What will that product include? How will the product be used? What is the schedule for completing the product?

# Considerations in Recommending Countermeasure Options

Communicating recommendations effectively to a customer is probably as important as the assessment itself. Faulty written or oral presentations likely will result in a failure to adopt what otherwise are worthy — minimum cost/maximum benefit — countermeasures. Analysts must make every effort to make their efforts clear, concise, and within those constraints, as complete as possible — avoid jargon and promote interest in what is being presented. When presenting recommendations to the customer, an analyst may use the following outline to structure the report or briefing.

1. Review the Purpose and Scope of the Risk Management Task with the Customer — capture the customer's attention by reviewing some recent event relevant to the assessment.
2. Present Findings
   - ▲ Review Assets: Which assets are critical and why? Explain loss impacts.
   - ▲ Review Specific Threats: What are they? Who are adversaries? Explain capability, intent, and history related to undesirable events.
   - ▲ Review Vulnerabilities: What are they? How do vulnerabilities relate to threats?
3. Present the Conclusions of the Assessment
   - ▲ Review Overall Risks and Priorities: What are the risks? Which risks are of greatest concern? Why? What might happen if they are not reduced?
4. Present Recommendations
   - ▲ Identify countermeasures: How much do the countermeasures reduce vulnerabilities/risks? What are the direct and operational costs? How will they impact end-users? What risks will remain after various countermeasure options are implemented?
   - ▲ What are the customer's responsibilities in selecting and implementing countermeasures? Why should the customer invest in recommended countermeasures? Why should the customer discontinue using existing countermeasures which are considered unwarranted?

# Worksheets and Charts

The following pages are blank copies of the Analytical Risk Management charts used as worksheets to facilitate the Risk Management process. They are included as a courtesy for use when employing the Risk Management methodology.

# Asset Assessment Chart

| Critical Asset | Potential Undesirable Event | Impacts | Impact Rating |
|---|---|---|---|
| | | | |
| People | | | |
| | | | |
| Information | | | |
| | | | |
| Equipment | | | |
| | | | |
| Facilities | | | |
| | | | |
| Activities/ Operations | | | |
| | | | |

# Threat Assessment Chart

| Critical Asset | Potential Undesirable Event | Threat/ Adversary | Threat Rating |
|---|---|---|---|
| | | | |
| People | | | |
| | | | |
| Information | | | |
| | | | |
| Equipment | | | |
| | | | |
| Facilities | | | |
| | | | |
| Activities/ Operations | | | |
| | | | |

# Threat Assessment Chart
## (Backup Data)

| Threat Category & Adversary | Intent (Motivation/ Need) | Capabilities (Methods) | History (Incidents/ Indicators) | Adversary Threat Rating |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Vulnerability Assessment Chart

| Critical Asset | Potential Undesirable Event | Vulnerability | Vulnerability Rating |
|---|---|---|---|
| | | | |
| People | | | |
| | | | |
| Information | | | |
| | | | |
| Equipment | | | |
| | | | |
| Facilities | | | |
| | | | |
| Activities/ Operations | | | |

# Risk Assessment Chart

| Critical Assets | Potential Undesirable Events | Impact Rating | | Threat/ Adversary | Threat Rating | | Vulnerability Description | Vuln. Rating | | Overall Risk | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

# Cost-Benefit Analysis Chart

| Undesirable Events | Countermeasures | Risk Level Reduced From/To | Cost | Comments |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Appendix A

## Creating Your Own Impact/Risk Scales

The scale you create depends on the definitions that you develop for the various points on that scale. These points may be described linguistically (e.g., a four point scale may be established with the following categories - - Critical, High, Medium and Low) or just numerically or a combination of the two. We recommend that the linguistic and numerical scales be related as noted below. A definition is a verbal description of the meaning of the linguistic term used in your scale (e.g., a Critical impact on your assets might be defined as: loss of life or mission failure). The scale should be exponential to describe the increasing severity of some Impact or Risk to your assets as you move up the scale. The steps for developing a scale are:

1. Establish the number of points you will use in your scale (e.g., Critical, High, Medium or Low) and define each of these terms.

2. Determine the end point of your scale e.g., 100.

3. Determine how many Highs (based on your definitions) are equivalent to one Critical e.g., you might determine that 2 Highs are equal to 1 Critical.

4. Divide the end point of your scale (e.g., 100) by the number of Highs (e.g., 2) you determine are equal to 1 Critical thus, for our example, 100/2=50. 50 is the initial point of the Critical category i.e., the Critical range is 50 to 100. To determine the exponential midpoint of that range: divide the higher number by the lower number, take the square route of the result; and then multiply by the lower number—e.g., 100/50=2, the square root of 2=1.41, and 1.41 X 50=70.1 and then rounding up gives you 72 as the midpoint in this example.

5. Determine how many mediums it takes to make a High (e.g., 4) and divide that number into the initial point of Critical (e.g., 50/4=12.5 or 13 when rounding up) gives the initial point of the High category. The High category's range in this example is 13 to 50. The exponential midpoint in this example is 25 (i.e., 50/13=3.84, square root of 3.84=1.96, and 1.96 X 13=25.47).

6. Determine how many Lows are equivalent to 1 medium (e.g., 6) and divide that number into the initial point of the High category (e.g., 13/6=2.17 or 2). Thus, the Medium category range is 2 to 13 and the midpoint of that range is 5 (i.e., 13/2=6.5, square root of 6.5=2.55, and 2.55 X 2=5).

7. The Low category is derived from the remainder but is never zero. In this example we might describe the Low range as .01 to 3 with a midpoint of 2.

For the example used above, the scale would look like this:

***This scale is used for Impact and Risk. For threat and Vulnerability use a probability scale.***

| | | |
|---|---|---|
| **Critical** | 50 to 100 | with a midpoint of 72 |
| **High** | 13 to 50 | with a midpoint of 25 |
| **Medium** | 3 to 13 | with a midpoint of 5 |
| **Low** | .01 to 3 | with a midpoint of 2 |

As noted, the scale has some broad ranges (e.g., 50 to 100) and that is why we suggest establishing midpoints. Doing this will provide a more granular approach when converting to or from the linguistic or numerical scales. For example, using the above scale a 72 linguistically would be a Medium/Critical, which in turn might describe a significant (but not catastrophic) loss of life and or potential for mission failure. A High/Critical (90 or better numerically) would describe a catastrophic impact.

# Appendix B

## Broadening the Linguistic Scale

*10 Choices Instead of 4*

We use a four point linguistic scale (i.e., Critical, High, Medium, and Low) and we have related each of these words to specific definitions. We also relate these terms to an exponential numerical scale when determining Impact of an undesirable event or when calculating risk. For example, the word Critical might relate to a numerical scale ranging from 50 to 100 on a 100 point numeric scale. As you can see, this is a broad numerical range for the word Critical to handle. Since we will convert the linguistic scale to a numerical scale to better calculate Risk and back to a linguistic scale for a better presentation of Risk, we suggest that you establish three levels of severity for each of the linguistic terms. For example, for Critical – Low/Critical (L/C), Medium/Critical (M/C), High/Critical (H/C). The same process, as noted below, should be used for High and Medium.

### Here's a sample scale used for Impact and Risk:

| | | |
|---|---|---|
| Critical | 50 to 100 | Midpoint is 72 |
| High | 13 to 50 | Midpoint is 25 |
| Medium | 3 to 13 | Midpoint is 5 |
| Low | .01 to 3 | Midpoint is 2 |

This scale is used for Impact and for Risk. For Threat and Vulnerability we use a linear scale to show probability. The concept of establishing linguistic degrees of severity for each linguistic category is the same for both scales.

Based on this table, a rating of M/C would be around 72 on the numerical scale. H/C would be somewhere in the nineties, while a numerical value of 50 to 60 would indicate a L/C Impact or Risk. A M/H would be somewhere around 25, a H/H in the 35 to 50 range, and a L/H from 13 to 20. M/M would be near 5, the H/M near 13, and L/M 3 or 4. It is unlikely that you would need this approach to show degrees of severity for the LOW category when rating Risk (R) or Impact (I), because of the low numerical range but you could using the examples already shown. *

Remember DC as a memory device for what comes first – Degree of severity within the Category. Thus, a High/Critical (H/C) means a High degree of severity within the Critical category (somewhere 90 to 100 on the numerical scale).

### In order the linguistics are:

H/C }
M/C } CRITICAL
L/C }

H/M }
M/M } MEDIUM
L/M }

H/H }
M/H } HIGH
L/H }

H/L }
M/L } LOW*
L/L }

# Appendix C

## Step – 5 Countermeasure Options and Cost Benefit Analysis

This is a suggested method for selecting and presenting three different countermeasure option packages to a decision-maker. The focus of the first package is on a Risk Averse, the second is Risk Prudent and the third is Risk Tolerant.

A. Select all of the countermeasures that apply to your specific situation that reduce the impact of a specific Undesirable Event. The CM worksheet # 1 should address all of the Undesirable Events and their respective CMs.

B. Group like CMs (such as locking devices, e.g. dead bolts, key pads, cypher locks and guard forces e.g., contract guards, SPOs, Marine Guards, ect…).

C. Enter all of the grouped CMs on the countermeasure worksheet # 1 with their associated costs.

D. Evaluate the general functional effectiveness (e.g. to deter, defend, delay, detect, deny, defeat or destroy) of each CM in reducing those Vulnerabilities that may lead to Undesirable Events. Use a scale of 1 (poor) to 10 (excellent). If the CM does not apply, leave the cell blank.

E. Use the CM worksheet # 2, Countermeasure Options Package, to develop a CM Options Package, as noted in F and H below.

F. Risk Adverse (maximum protection) Package. Select those CMs that are most effective. Ensure that all CM protective functions are covered (e.g. to deter, defend, delay, detect, deny, defeat or destroy). For the most Critical risks (based on your assessment), consider redundant CMs. Ensure all Critical, High and Medium risks are covered. Note the Options Package you are working on and record your CM selections on CM worksheet # 2.

G. Risk Prudent (recommended) Package. Select those CMs with the highest effectiveness and the lowest cost. Ensure that most CM protective functions are covered. Based on your risk assessment, address all of the Critical and High risks. For the most Critical risks, consider redundant CMs. Note the Options Package you are working on and record your CM selections on CM worksheet # 2.

H. Risk Tolerant (least expensive) Package. Select those CMs that are lowest in cost and yet address what you believe to be the most Critical risks (based on your risk assessment) and minimally provide some deterrence value to those Critical risks. Note the Options Package you are working on and record your CM selections on CM worksheet # 2.

I. For the presentation of your CM options and to provide another check of your CM selections, consider using the Countermeasure Worksheet # 3.

# Countermeasures Work Sheet #1

*Countermeasures' Analysis for Undesirable Events*

| Undesirable Event | Countermeasure | Cost | Defeat/Destroy | Deny/Defend | Delay | Detect | Deter |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Scale for Protection Functions of CMs: Poor 1 to Excellent 10. Blank is N/A**

# Countermeasures Work Sheet #2

*Countermeasures' Option Package*

| Undesirable Events (1) | Existing Risk (2) | Related Vuln. Level & Vuln. (3) | Countermeasures (4) | Cost (5) | New Vuln. Level (6) | New Risk Level (7) |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Existing Risk → | | | Total Cost → | | New Risk Level → | |

**Column Notes: V = Vulnerability; T = Threat ; I = Impact; R= Risk**

(1) Specify each event (2) Enter the rating from your Risk Assessment Worksheet (3) Enter old V or T or I ratings affected by your new CMs from your Risk Assessment Worksheet (4) ID your new additional selected countermeasure from CM Worksheet #1 (5) Enter its cost (6) Enter the new V or T or I rating that results when you use the new CM (7) Calculate and enter the new risk level [R=IxTxV] when you use the new vulnerability level of column (6). The bottom row provides the total cost for all CMs and shows from/to risk data.

# Countermeasures Work Sheet #3

*Countermeasures' Analysis for Undesirable Events*

| Undesirable Events | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Countermeasure** | **Cost** | | | | | | | | | | | | | **CM Effect** |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| **Current Risk Level** | | | | | | | | | | | | | | |
| **Risk After CM** | | | | | | | | | | | | | | |

# Glossary of Terms

**Adversary**: Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. An ***adversary*** could include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, and private interests.

**Analytical Risk Management (ARM):** The process of selecting and implementing security ***countermeasures*** to achieve an acceptable level of ***risk*** at an acceptable ***cost***.

- A structured yet flexible approach to understanding your security posture.
- A process for developing effective security countermeasures and options that consider cost & benefit.
- A snapshot in time that provides an audit trail.

**Asset:** An ***asset*** is any person, facility, material, information, or activity which has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets may be categorized in many ways. Among these are:

- People
- Information
- Equipment
- Facilities
- Activities/Operations

**Benefit:** Amount of risk reduction based on the overall effectiveness of countermeasures with respect to the assessed vulnerabilities.

**Capability:** When assessing the ***capability*** of an adversary, one needs to two distinct categories to evaluate. The first is the capability to obtain, damage, or destroy the asset. The second is the adversary's capability to use the asset to achieve their objectives once the asset is obtained.

**Cost:** Includes tangible items such as money and equipment as well as the operational costs associated with the countewrmeasures' implementation. There are also intangible costs such as lost productivity, morale considerations, political embarrassment and a variety of others.

**Cost-Benefit Analysis:** Part of the management decision-making process in which the costs and benefits of each countermeasure alternative are compared and the most appropriate alternative is selected. Costs include the cost of the tangible materials, and also the on-going operational costs associated with the countermeasure implementation. Benefits are expressed in terms of the amount of risk reduction based on the overall effectiveness of the countermeasure with respect to the assessed vulnerabilities. The risk management process is designed to provide the most benefit for the least cost.

**Countermeasure:** An action taken or physical entity principally used to reduce or eliminate one or more ***vulnerabilities***. The countermeasure may also affect ***threat*** (intent and/or capability) as well as the asset's value. The cost of a ***countermeasure*** may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

**Impact:** The amount of loss or damage that can be expected, or may be expected from a successful attack of an asset. Loss may be monetary but may also include political, morale, operational effectiveness, etc. impacts.

**Impact of Loss:** The value placed on that ***asset*** by its owner and the ***consequence***, ***impact***, or adverse effect of loss or damage to that ***asset***.

**Intent:** When assessing threats, security professionals need to evalaute intent as well as capabilities. To determine the intent and what motivates an adversary, look closely at an adversary's goals and objectives, as well as specific events that might trigger the adversary to act. Ask yourself, ìDoes the adversary have a current or projected needfor this asset? Do they seek to deny or destroy the use of the asset?

**Linguistic Scale:** TBD

**Numeric Scale:** TBD

**Probability of Adverse Event:** The ***likelihood*** that a specific ***vulnerability*** will be exploited by a particular threat.

**Risk:** The potential for damage to or loss of an ***asset***. The level of ***risk*** [R = I (***impact***) x T(***threat***) x V (***vulnerability***)] is a combination of two factors:

1. The ***value*** placed on that ***asset*** by its owner and the consequence of an ***undesirable event*** on that ***asset*** - the ***impact*** (I) in terms of adverse effect or loss or damage to the ***asset***.
2. The likelihood that a specific ***vulnerability*** (V) will be exploited by a particular ***threat*** (T).

**Risk Level:** Is a combination of the two factors pertaining to ***impact of Loss*** and ***probability of adverse event***.

**Risk Management:** The process of selecting and implementing security ***countermeasures*** to achieve an acceptable level of ***risk*** at an acceptable cost.

**Risk Assessment:** Risk (R) assessment is the process of determining the likelihood of an adversary (T) successfully exploiting a vulnerability (V) and the resulting degree of damage or impact (I) on an asset. A risk assessment provides the basis for rank ordering risks and thus establishing priorities for the application of countermeasures. Thus the formula of R = I x (T x V) is used.

**Threat:** Any indication, circumstance, or event with the potential to cause the loss of, or damage to an ***asset***. ***Threat*** can also be defined as the intention and ***capability*** of an ***adversary*** to undertake actions that would be detrimental to critical assets. There are six principal sources of ***threats***, see ***threat categories***.

**Threat Categories:** Include; insider, terrorist, intelligence service, criminal, military and environmental.

**Undesirable Events:** Undesirable events provide a guide for what we need to protect against. After identifying and prioritizing assets, one must seek to obtain what unwanted events could possibly have an impact on the assets. Analysts must look at the past, present, or even to other organizations assets to identify what could affect their assets in the future. Undesirable events result in a loss to the asset, whether it is a loss of capability, life, property, or equipment.

**Value:** In the ARM process, value is assigned with both a linguistic and numeric scale. This placing of assigned value helps to define the overall level of risk. Value is placed on each of the three elements thereof, i.e. (Impact, Threat, and Vulnerability). Value is assigned in the following terms:

- Critical 50 - 100
- High 13 - 49
- Medium 4 - 12
- Low 1 - 3

**Vulnerabilities:** Any weakness that can be exploited by an ***adversary*** to gain access to an ***asset***. Vulnerabilities can include but are not limited to building characteristics, Equipment properties, personal behavior, locations of people, equipment and buildings, or operational and personal practices.